Data Flow and Access Control Policy Models in Wireless Body Area Network for Healthcare

A THESIS SUBMITTED TO
THE SCIENCE AND ENGINEERING FACULTY
OF QUEENSLAND UNIVERSITY OF TECHNOLOGY
IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF INFORMATION TECHNOLOGY (RESEARCH)

Ahmad Salehi Shahraki

Principal Supervisor: Dr Seyit Camtepe
Associate Supervisor: Dr Dhammika Jayalath

Science and Engineering Faculty
Queensland University of Technology

2016

Abstract

Body area networks (BAN) represent an emerging technology that focuses on monitoring physiological data in, on and around the human body and that supports different applications of implanted sensors and wearable wireless sensor devices. BAN technology permits wearable and implanted sensors to collect vital data about the human body and to transmit them to other nodes (e.g., a smartphone or tablet) via low-energy communications using over-the-air radio frequency. Many companies and universities throughout the world have suggested numerous BAN applications in electronic healthcare services. To achieve the maximum benefit of healthcare services, shared health information must be sequentially processed in real time. Critical data may be accessed by various user groups such as physicians, other healthcare providers and patients in the hospital, at home and other places. This technology should help improve the quality of life for patients and provide a variety of services with medical applications. Recent developments in mobile computing and communication permit patients to move freely and to be monitored at any location at any time. However, existing studies on data flow communication models focus only on individual patient monitoring in indoor environments such as hospital or home. Healthcare and remote healthcare monitoring of small and large groups in indoor and outdoor environments have not been reported thoroughly in the open literature.

This thesis starts with an investigation of the interactions in terms of data flow between parties involved in BANs under four scenarios targeting outdoor and indoor medical environments: hospital, home, emergency vehicle and open areas. Using these scenarios, data flow requirements identified between BAN elements such as sensors and control units and parties involved in BANs such as patients, doctors, nurses and relatives. Identified requirements are used to generate BAN data flow models under indoor and outdoor healthcare environments. Petri Nets (PNs) are used as the formal modelling language. We checked the validity of the models by simulating data flow models based on PNs. Finally, these models and key ideas of

information security and the privacy of shared sensitive data over open networks were used to design a policy model that would allow different parties to access medical resources securely. This policy model permits different authorities to manage various requests from the inside and outside areas. To support and exchange the policies, a workflow framework was created based on the concept of eXtensible Access Control Markup Language, which is appropriate standard to provide access control policy model.

Table of Contents

List of Figures

List of Tables

Copyright in Relation to This Thesis

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature:

Date: 25/10/2016

To my family

Keywords

Access Control, Body Area Networks (BANs), Data flow, Healthcare monitoring, Sensor, Security, Policy, and Policy Language Model.

Acknowledgments

Pursuing a university degree is a challenging experience, and one of the keys to success is the support of supervisors, colleagues, friends, and family. Now that my masters degree has come to an end, it is a pleasure to thank the many people who made it possible.

I would like to extend my special thanks to my principal supervisor, Dr. Seyit Ahmet Camtepe, for his excellent guidance, constant encouragement, patience and care during my entire course of study. Also, I am also grateful to my associate supervisor, Dr. Dhammika Jayalath, for his excellent guidance, constant encouragement, patience and care during the entire course of this study.

Thanks also to Dr. Ernest Foo, A/Prof. Dian Tjondronegoro and Dr Inma Tomeo-Reyes for their constructive and valuable feedback during my study. I am also grateful to Professor Josef Pieprzyk, Professor Colin Fidge, Professor Xavier Boyen, Professor Vinod Chandran, Professor David Lovell, Dr Tony Sahama, Dr Douglas Stebila, Dr Kenneth Radke, Dr Vicky Liu, Dr Praveen Gauravaram and Dr Deborah Peach for their appreciation and constructive feedback and help during my study in QUT.

I also thank my colleagues and friends at QUT, who made my working life much easier and enjoyable. I would especially mention Nasir Hussain, Ben Dowling, Nicholas Rodofile, David Myers, Qinyi Li, Thomas Haines and Janaka Alawatugoda.

I acknowledge Queensland University of Technology Postgraduate Research Award (QUT-PRA) and Higher Degree Research (HDR) tuition fee award for providing the scholarship to pursue my masters studies. Copyediting of this thesis was performed by Dr. Laurel Mackinnon and is acknowledged according to universitys guidelines laid and endorsed by the national policy guideline for the editing of research.

Finally, I would like to thank my wife for her continuous support of my masters experience

and my father, mother, brother and sisters for their moral support and their support as I live far away from them all.

Preface

This thesis is submitted to the Queensland University of Technology (QUT) in partial fulfilment of the requirements for the degree Master of Information Technology (IT). The work has been conducted at the faculty of Science and Engineering, Department of Electrical Engineering, Computer Science (EECS) and information security discipline, under supervision of Dr Seyit Camtepe and Dr Dhammika Jayalath.

Abbreviations

AA	Attribute authority
BAN	Body area networks
BS	Base Station
CH	Cluster head
CH	Context handler
CU	Control unit
DP	Department
DR	Doctor
ECG	Electrocardiogram
EMG	Electromyogram
EN	Environment
EEG	Electrocardiography
ENVS	Environmental sensor
HBC	Human body communication
HOS	Hospital
HOM	Home
ISM	The industrial, scientific and medical
IMD	Implantable medical device
MANET	Mobile Ad hoc network
MAC	Message authentication code
MCD	Mobile Computing Device
MICS	Medical Implant Communication Service
NUR	Nurse
NFC	Near field communication
NB	Narrowband
OP	Open area

PRP	Policy retrieval point
PAP	Policy administration point
PDP	Policy decision point
PEP	Policy enforcement point
PIP	Policy information point
PDA	Personal digital assistant
PN	Petri Nets
PA	Permission assignment
RBAC	Role-based access control
RF	Radio frequency
REQS	Request for service
RESS	Response service
RFID	Radio frequency identification
RH	Role hierarchy
SEN	Sensor
SCC	Strongly Connected Components
TMD	Telemedicine Device
TG6	Task Group 6
UWB	Ultra-wideband
UA	Users assignment
UML	Unified Modelling Language
WBAN	Wireless body area networks
WSN	Wireless sensor network
WPAN	Wireless personal area network
WLAN	Wireless local area network
WMTS	Wireless Medical Telemetry Services
WSS	Wearable Sensor System

XACML EXtensible Access Control Markup Language

Chapter 1

Introduction

The background of the research project is presented in Section 1.1. This is followed by the research problem and aim of this research project in Section 1.2. Section 1.3 includes the research questions and objectives, Section 1.4 outlines the research project and Section 1.5 outlines the research scope and significance, and Section 1.6 outlines the organization of this thesis.

1.1 Research Background

An increasing number of people are demanding electronic healthcare services. These services and supporting technologies have evolved within the context of body area networks (BANs). BANs are an emerging technology that is playing a major role in healthcare applications. BANs are similar to wireless BANs or wireless sensor networks, which use wireless radio frequency (RF)-based communication. BANs comprise mainly wearable sensors (e.g., for heart rate, temperature, electrocardiogram, blood pressure, motion detection, and pulse oximetry) that are worn on or implanted in the body and a control unit (CU) [Kumar and Lee, 2011]. Sensors are designed and configured to collect physiological data about the human body at any time and any place while the body is in motion or is in sleeping and sitting motionless. Each sensor node transmits data to the CU, which works as a gateway interface for the sensors. The CU collects, aggregates and forwards the data to be recorded by a medical server so that it can be accessed by a physician or other healthcare service provider such as another doctor, nurse or insurance company. This allows users to access shared sensitive data from any place at any time. By using

BAN technology, users and other stakeholders can monitor personal data remotely in real time [Chen et al., 2011].

BAN elements such as sensors and the CU use a radio connection to communicate. BANs can also communicate with other BANs. Each BAN may use a different wireless communication technology that operates at a different frequency (e.g., 2.4 GHz The industrial, scientific and medical (ISM)) to transfer data from inside to outside or vice versa. The choice of the communication technology depends on the application requirements such as the data rate and communication range [Acampora et al., 2013]. BANs may interact with other existing wireless technologies such as ZigBee, Bluetooth and RF identification. In contrast to the limits imposed by existing technologies, BANs allow a patient to move from the hospital and continue to be monitored for a long time, at home or elsewhere. This technology can support and reduce the cost of healthcare service [Khan et al., 2008].

The cost of healthcare services motivates researchers to provide accurate healthcare data in real time to enhance the patient's quality of life. The increase in population throughout the world increases the cost of healthcare services. For example, in Australia, life expectancy increased around 14.75%, from 70.82 years in 1960 to 82.10 years in 2012. In the USA, life expectancy increased around 12.8%, from 69.77 years in 1960 to 78.74 years in 2012. In Canada, life expectancy increased around 13.27%, from 71.13 years in 1960 to 81.24 years in 2012. The increasing demand on healthcare services by an increasingly aging population is a critical issue. The cost of healthcare services has risen increasingly in recent years. Research shows that the ability of healthcare provider services to detect health problems in real time improves patient's health outcomes and quality of life [Custodio et al., 2012].

As outlined above, BANs can be used to monitor how people manage their health, how BANs interface with other networks, and how vital data are transferred from the human body to other places for further services. However, patients also need strong security and privacy as well as adaptability and safety to improve quality of healthcare service which these services provide better life [Movassaghi et al., 2014]. A number of approaches such as traditional cryptography, physiological signalling and physical layer security have been proposed to improve the security of the medical devices in individual BANs. These approaches have been tried in indoor and outdoor areas such as homes and hospitals, but these approaches cannot satisfy the security requirements of BANs. Better healthcare services require strong security and a reliable and

adaptable communication model that can be used to share health information among different parties. The overall aim of this research project is to identify and understand the requirements for a communication system to transmit health data within and between BANs in a variety of applications in health. Wide deployment of BANs in health and other domains require the development of efficient solutions made specifically for BANs and their application domains [Chen et al., 2011].

1.2 Research Problem and Aim

The key challenge in the healthcare area is to meet the requirements of different parties and to deliver the most benefits that data and services can provide for improving the quality of electronic healthcare services. Healthcare service providers need to access health data in real time to monitor their patients at any place and time. To achieve this, BANs have become an attractive topic for many application domains including healthcare services at home, hospital and other places. Medical data transfer between various stakeholders in different areas is based on RF technologies. Therefore, wireless healthcare applications present many new challenges including communication and computation, mobility of nodes in medical areas, reliable communication for data transmission, energy consumption, patient management, security and privacy. To deploy BANs successfully and safely, BAN applications have certain requirements. Appropriate data flow models based on different roles, policies, communications, protocols, technologies and topologies are required. Practical policy models based on data flow models also must be developed to verify the data flow models developed in this research project.

Generally, the capture of vital physiological signals of individuals or groups using BAN technology is a challenging issue. Recent developments in mobile computing and communication permit patients to move freely and be monitored at any location at any time. However, existing studies on data flow communication models focus on individual patient monitoring in indoor environments such as the hospital or home. Huang et al. [2009], proposed a general healthcare model to monitor small groups of patients in indoor environments. However, healthcare and remote healthcare monitoring of small and large groups in indoor and outdoor environments have not been addressed. Moreover, in traditional sensor settings, sensors send their measurements to CUs periodically or whenever an incident happens. As opposed to this one-way data flow, in a two-way data flow, CUs may also send codes, queries or data to

sensors to filter, aggregate, relay or cache data to decrease communication overhead and energy consumption and improve security. In the absence of well-established intra- and inter-BAN data flow models in healthcare monitoring, communication and BAN requirements may not be understood properly. Data flow models in healthcare settings are required to understand the relationships between patients, healthcare service providers and other elements. Furthermore, suitable data flow models are important in the healthcare setting to collect health data as an input and to understand how health data are transmitted between parties and how particular components are handled. Therefore, a highly detailed model of the health system and the required security is needed. These security requirements are essential to the design of appropriate security and privacy mechanisms. This constitutes an important factor that may reduce usability and acceptability of BAN-related products in the health domain.

1.2.1 Research aim

The aims of this research were to understand the key players, data flow, access control policy and communication requirements in inter- and intra-BAN communication, and to develop appropriate data flow and access control policy models to meet security requirements.

1.3 Research Questions and Objectives

The key question of this research project was: What are the best models to transmit health data in inter- and intra-BAN communication in a variety of applications in health? Motivated by the arguments presented above, this thesis had the following research objectives:

1. To investigate and analyse WBANs in the healthcare domain.
2. To develop and verify data flow models for BAN applications in healthcare domains.
3. To develop an access policy model for BAN data flow models.

1.4 Research Outcomes

In this research project, we investigated the interactions in terms of data flows between parties involved in BANs under four different scenarios that targeted outdoor and indoor medical

environments: hospital, home, emergency and open areas. We focused on healthcare and remote healthcare monitoring of individuals and large patient groups. We considered centralized and decentralized scenarios and investigated the effects of medical procedures, rules and policies in BANs. Our work was not limited to one-way communication from sensors to CUs but also considered possible two-way communication schemes in which CUs can send queries, data and codes to sensors. Based on these scenarios, we identified data flow requirements between BAN elements such as sensors and CUs and other parties involved in BANs. The requirements identified were used to generate BAN data flow models.

The first step was comprehensive literature review to establish the background of the research problem, to identify gaps in knowledge and scope, and to validate the research methodology. Based on the initial research proposal, Chapter 2 includes an extensive literature review. To develop a data flow model, different BAN application domains and scenarios for each medical domain were identified. Based on the different domains and applications, a variety of stakeholders, such as patients, doctors, nurses, family members and insurance companies, were investigated and identified in relation to each model. Different rules and responsibilities of each stakeholder were introduced based on each domain. The BAN architecture and security model were also introduced and modelled, and a data flow model for BAN communication under four healthcare environments (hospital, home, emergency and open areas) was created. Unified Modelling Language was used to examine the model developed based on the different parameters, which is described in Chapter 3. The data flow model using Petri Nets (PNs) software was also examined. PNs was used as the formal modelling language to check the validity of the models and to compare them with the existing related work. The types of indoor and outdoor attack scenarios on data flow were identified and are presented in Chapter 3.

According to the data flow model developed for indoor and outdoor areas, the patient-related data are shared between different healthcare environments and healthcare service providers. The authority of domains predefine some policies and give some permission to users to access the system from any place and time. It is recommended that the policy model and framework with respect to different attributes from the subject, object, environment, situation and their recourse use the concept of eXtensible Access Control Markup Language (XACML). XACML is a standard language based on access control policy language. The access profile is designed to control the users under a predefined policy controlled by the administrator of a specific healthcare system. The history of all actions, such as access, previous permission and location

of the requester, is recorded, and this can help the administrator develop better access control policies. The concept of role-based access control provides the access profile and permission to filter the new policies, while policies defined with system. Finally, the access control policy model based on the presented data flow models is developed using XACML.

This research project provides information about healthcare application issues and technologies that support large-scale networks. Significant security, privacy and safety issues may prevent the widespread adoption of these technologies. Because of the transmission of critical data over the air, patients may be harmed by attacks by an unauthorised user, authorized people or false data injected into the network. The significance of this study lies in its development of medical network architectures to provide better remote healthcare monitoring of individual and large patients groups in indoor and outdoor environments within BAN communication. This research addressed an important healthcare concern: improving the quality of healthcare services and, indirectly, the quality of life of patients. The main scope of this research is to develop outdoor and indoor healthcare models to monitor the state of patients in real time. This helped identify how input and output data are transmitted over an open network between different parties. The results presented are based on developed models and show that these models are useful in BAN applications in health settings. The models show that how data transmit from input to the result of model as an output. In addition, this research provides an access control policy model based on developed data flow models created using the concept of XACML. The models developed show that the health data can be updated automatically and recorded in a medical database, and the users can read and monitor the patient's complete health summary in real time. Recording these health data within the system should help to reduce the cost of healthcare services.

- Publications:

1- Conference paper:

Ahmad Salehi S., Seyit Camtepe and Dhammika Jayalath, ”Understanding Data Flow and Security Requirements in Wireless Body Area Networks for Healthcare,” In IEEE 17th International Conference on E-health Networking, Application and Services (IEEE Healthcom’15), USA, 2015

1.5 Research Scope and Significance

The primary aim of this research is to develop appropriate data ow and access control policy models to meet security requirements in BAN. One of the techniques in ensuring the correctness of a data flow model is to investigate and understand the key players, data ow, access control policy and communication requirements in inter- and intra-BAN communication. Policy models based on a healthcare environment are unlike other security solutions in sensor networks; security in WBAN in the health domain is context dependent; security involves multiple parties assuming time and location dependent roles (who can have what type of access to which objects owned by whom at which location and what time). In addition to this complexity, the absence of a trusted centralized authority forms a major technical challenge in developing security protocols that meet the WBAN eHealth security requirements. Hence, the contribution of this thesis in data flow and access control policy models, forms the foundation for existing and future WBAN eHealth security solutions. As a result, this research focused on communication in inter- and intra-BAN to develop outdoor and indoor data flow models to help to monitor the state of patients in real time. Formal models of a data flow model, based on the Petri Nets specication, are required because there are no existing models, or known simulations that are available for data flow in indoor and outdoor areas to check and validate the developed model. In addition, to provide a suitable access control model to represent a patients situation, an access control framework and policy model is required to evaluate subjects based on their attributes and duties. The XACML language is used with the authorisation model to evaluate the developed framework. In addition, the signicance of this study includes:

- Development of network architecture to provide better remote healthcare monitoring of individual and large patient groups in indoor and outdoor environments within BAN communication.

- The developed architecture in this research helped identify how input and output data are transmitted over an open network between different parties.

- The research presented in this thesis will help system designers to develop deeper understanding of the underlying WBAN for their requirements and security.

- The outcomes of this research will help system designers in developing appropriate security and privacy mechanisms to protect shared data over an open network.

- The outcomes of this research will provide signicant contributions towards reducing the cost of healthcare services and also provide a basic network for WBAN communications.

- The empirical and analytical investigation of this study would be very useful for the design, implementation and deployment of present and future WBAN environments.

1.6 Thesis Outline

i. Chapter 1 of this thesis introduces the program of research and includes an overview, background, research objectives, research questions, research outcomes and their significance, and thesis outline.

ii. Chapter 2 reviews the literature on BANs and the model proposed in this research study. This chapter presents a classification, summary and critical evaluation of existing work and proposed models relevant to the research problem in this study.

iii. Chapter 3 develops a data flow model based on architecture in different healthcare environments in this research project.

iv. Chapter 4 describes an access control policy model that is based on the data flow models developed.

v. Chapter 5 outlines the main findings of this research and lists potential further issues for future research.

Chapter 2

Literature Review

This chapter analyses the literature on body area networks (BANs) related to the healthcare domain. There is an extensive literature on BANs and, in several cases, the studies overlap. The main goal of this chapter is to present a comprehensive literature review as background to the research on BANs and to evaluate and analyse the literature related to this research project.

2.1 Background of BAN

Modern healthcare-related BANs can be developed by using wireless sensor networks (WSNs) to introduce wearable and implanted sensor networks for healthcare monitoring [Sohraby et al., 2007]. Energy efficiency and lower costs improve the performance of computing, communication and memory resources via current embedded systems [Asada et al., 1998]. Homogeneous and heterogeneous autonomous devices in BAN communication can be linked by WSNs [Akyildiz and Vuran, 2010, Movassaghi et al., 2014].

A BAN is an emerging technology that involves a wireless network of wearable computing devices with the aim of improving the quality of healthcare services and thus improve patients quality of life. A BAN is defined as a wireless network of heterogeneous computing devices that are wearable, which makes possible the continuous remote monitoring of a patient's physiological data in the medical setting [Movassaghi et al., 2014]. Our research is concerned mainly with BANs, which typically include two types of devices: sensors and a control unit (CU, sink). Sensors are configured to sense the body's physiological data. The CU works as gateway between attached devices in or on the body and other devices such as access points to forward

related data to the medical server. Figure 2.1 shows a BAN with sensors that are placed at various locations on the body and that support multiple network topologies by forwarding the sensed data to a medical server through a more computationally powerful device such as a smart phone or a personal digital assistant (PDA). Healthcare service providers can then access medical data remotely via the internet and cloud to monitor the state of a patient in real time [Wan et al., 2013].

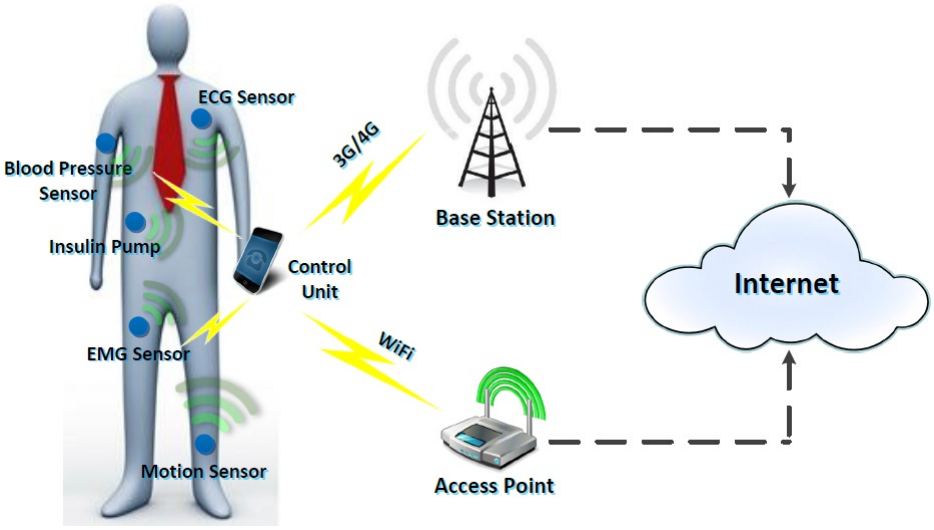

Figure 2.1: Variable medical Body Area Networks
[Brown, 2012, Wan et al., 2013]

2.1.1 Types of Nodes Used in BANs Communication

A node can perform some processing, collect data and communicate with other nodes in small- or large-scale networks. This section describes the classification of nodes in terms of their functionality.

Implant node: An implant node is planted in or under the skin (3 cm) to monitor vital data over a long time. The programmer is an external device that uses a wireless interface such as radio frequency (RF) to send and receive data [Zhang et al., 2014a].

Sensor: A sensor is a device (key component) that is attached within or outside of the body. Sensors are configured to sense physiological data from the body and to transfer the data to a CU (personal device) through a wireless medium. These devices allow the monitoring of vital data from the body at any time and place. Some existing types of sensors are listed and

described in Section 2.1.2 [Felisberto et al., 2012].

Control Unit (CU): A CU or personal device (PD) collects related data from body sensors in or around the body and forward them to medical server. The CU works as a gateway between sensors attached within or on the body and any external devices. The components in a CU are a processor, power, transceiver and memory. The CU must have a faster processor and a high-capacity battery. Smartphones and PDAs are examples of CUs used in BANs.

External Node: An external node is used in the vicinity of the human body such as an access point, cellular phone or a computer. An external node can be installed within a few centimetres (and within 5 m) of the body. The external node transfers data between the CU and healthcare service providers. The advantages of an external node over an internal node are increased power and memory.

In addition, A number of researchers have used from 0 to 256 nodes in each BAN for transmitting related data. Based on BAN architecture, each CU can support 64 nodes. The following factors are important considerations for BANs with more than 64 sensors: 1) communication protocol, 2) transmission technology, 3) network architecture, and 4) application. In addition, the type and number of nodes in BAN communication can change based on interactions between BANs in the same environment [Ullah et al., 2012].

2.1.2 Hardware

Sensor devices in BANs comprise two parts: physiological signals and radio platforms. Generally, a body sensor collects the analogue signals from the body, converts them to digital signal and then transfers them to other devices through radio platforms such as ZigBee. This section describes some of the existing hardware and devices used in BANs.

- **BAN Sensor:**

BAN sensors are an important part of BANs, and their size, task and adaptability are critical issues in health applications. As mentioned in Section Background, sensors gather the vital data from the body and forward the data to a medical server through a CU for further services. Sensors commonly used in BANs are listed and their features compared in Table 2.1. A brief description of each sensor is provided below the table.

Table 2.1: Type of Sensors in BANs

[Latré et al., 2011]

sensor	Energy	BER	Latency	Rate of bit	Duty cycle	QoS	nodes	Set up times	Topology	privacy	Data rate
Accelerometer	Low	10^{-10}	<250ms	<10kbpa	<1%	Yes	<12	<3s	Star	High	High
Blood glucose	Extremely low	10^{-10}	<250ms	<1Mbpa	<1%	Yes	<12	<3s	Star	High	High
Blood pressure	High	10^{-10}	<250ms	<10kbps	<1%	Yes	<12	<3s	Star	Medium	Low
CO gas sensor	Low	—	<250ms	<10kbpa	<1%	Yes	<12	<3s	Star	High	Very Low
electroencephalogram	—	10^{-10}	<250ms	86.4kbpa	<10%	Yes	<6	<3s	Star	—	High
Electrocardiogram	Low	10^{-10}	<250ms	<192kbpa	<10%	Yes	<6	<3s	Star	High	High
Electromyography	—	10^{-10}	<250ms	<10kbpa	<1%	Yes	<12	<3s	Star	High	High
Humidity	—	10^{-10}	<250ms	<250kbpa	<10%	Yes	—	<3s	Star	—	Very Low
Temperature	—	10^{-10}	<250ms	<10kbpa	<1%	Yes	—	<3s	Star	—	High
Image	Low	10^{-3}	<250ms	<100kbpa	<50%	Yes	2	<3s	p2p	Medium	Very High
Video	Low	10^{-3}	<1000ms	<100kbpa	<50%	Yes	2	<3s	P2P	Medium	Very High
Audio	High	10^{-5}	<100ms	1Mbpa	<50%	No	3	<3s	Star	Low	Low

Blood pressure: Blood pressure sensors provide a non-invasive method for measuring diastolic and systolic blood pressure, two of the principal vital signs in the human body.

Electrocardiogram (ECG): Electrocardiogram (ECG) sensors record heart activity and direct the signals to a medical server for monitoring by a physician. A number of ECG sensors are attached to the skin to monitor these signals.

Accelerometer: Accelerometers helps the physician monitor patient posture (e.g., crawling, running). Accelerometer sensors are also used in other applications such as entertainment and games.

Electromyogram (EMG): Electromyogram (EMG) are used for neuromuscular monitoring while the patient is at rest. EMG is used to avoid post-operative residual curarization.

Carbon dioxide (CO_2) gas sensor: Carbon dioxide (CO_2) gas sensors calculate the gaseous CO_2 level and can be used to monitor the oxygen concentration in the blood.

Electrocardiography (EEG) sensor: Electrocardiography (EEG) sensors record brain activity. The data are sensed and redirected to an amplifier for processing.

Blood glucose: Blood glucose sensors monitor the amount of glucose in the human blood.

Temperature sensor: Temperature sensors calculate the temperature of the human body and environment.

Humidity sensor: Humidity sensors are used to calculate the humidity of different environments.

Based on the different scenarios in which BANs can be used, such as open areas, relevant patient data must be monitored in real time and transferred to a medical database for further

services. Data can be available in two ways. Firstly, the body sensor collects physiological data and pushes them to the cloud or the internet by using a smartphone or any device that supports 3G, 4G or similar technology. Secondly, some commercial cloud sensor devices such as Libelium can collect and transfer physiological data over the air via 3G. This sensor is equipped with a new communication model that uses 3G and 4G technologies for remote management [Shaikh et al., 2015, Zhou, 2012].

2.1.3 Position of BAN

Research and development in the domain of BANs has a short history. The advanced protocols for BANs span from communication between sensors and body nodes to a data centre. The proposed definitions, including both intra-BAN and inter-BAN communication, can generate a clear understanding. Figure 2.2 shows an example of intra-BAN communication used to check information management on the body (e.g., between sensors and personal devices) where a multi-tiered telemedicine system is presented. Each tier displays different types of communication: tier 1 comprises intra-BAN communication (e.g., in/on sensors), tier 2 comprises inter-BAN communication (e.g., smartphone, tablet) and tier 3 comprises inter-BAN communication (e.g., internet and cloud). The combination of tier 1 and tier 2 communications can enable dispersed healthcare services and ensure secure communication between all devices in the BAN. A physician can receive medical data from the patient remotely and provide a consultation or store the data in a medical database [Latré et al., 2011].

At the present time, various system architectures and service platforms for inter-BAN communication are being considered for development. BANs for medical applications require sensor devices that monitor data from the body and transfer the data to a medical server. Figure 2.2 shows the similarities and differences between different wireless networks such as wireless body area networks (WBANs), wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks and wireless wide area network. The communication in BANs is in close range (e.g. 12 m) around the body, whereas the range in WLANs is more than 100 m. All networks include specialised technologies such as ZigBee and Bluetooth. These are explained in detail in Section 2.5 [Latré et al., 2011], [Hughes et al., 2012].

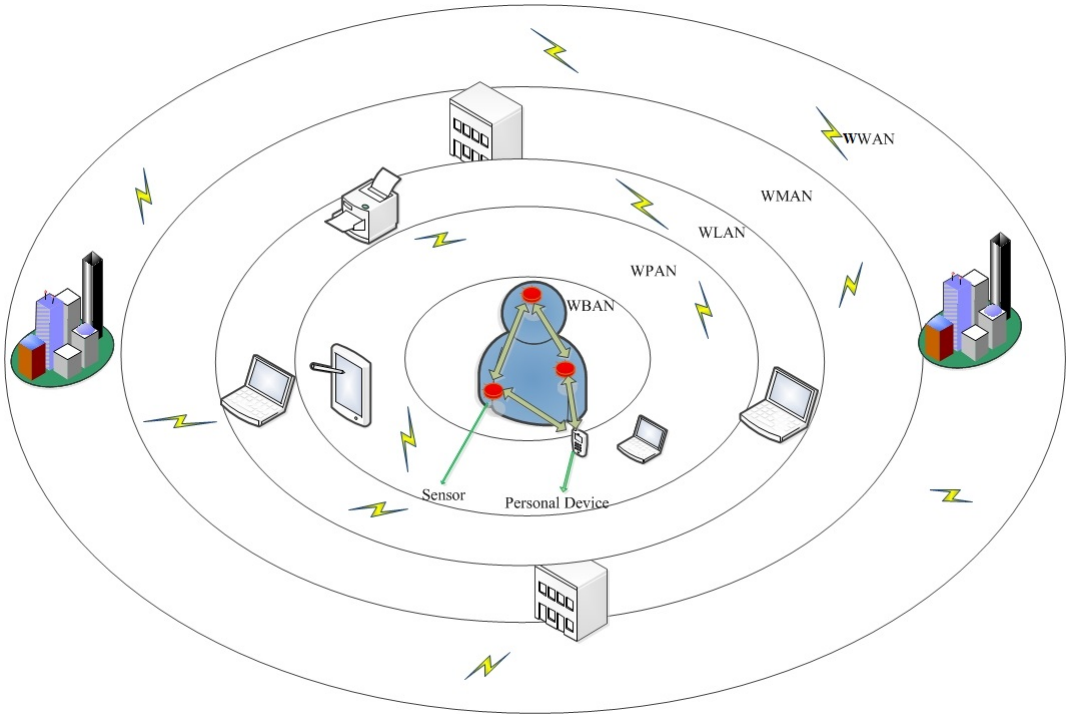

Figure 2.2: Positioning of a Body Area Network

2.2 BAN Applications

2.2.1 Current Applications of BANs

BANs can be used in diverse fields including healthcare, entertainment and games, fitness, defence, medicine, consumer electronics and emergency services. BAN applications allow radio connection to sensors and devices for purposes such as monitoring the vital signs of the body including electrocardiography, blood monitoring, and detecting motion [Drude, 2007], [Wong et al., 2013]. The applications of BANs can be divided into three categories: 1) in-body applications, which include implanted devices such as pacemakers; 2) on-body medical applications, which include wearable sensors such as those to detect temperature or for electrocardiography; and 3) on-body non-medical applications, which include entertainment and sports sensor devices. These sensors/devices (in-body or on-body) monitor the state of the body and transmit data to a medical server in hospitals for use by healthcare service providers [Movassaghi et al., 2014], [Ullah et al., 2010]. A sample BAN application model is presented in Figure 2.3. Different types of BAN applications and sensors are described in Table 2.2.

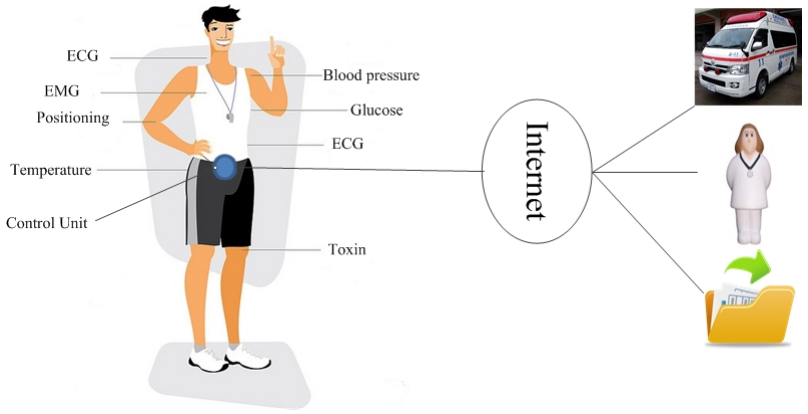

Figure 2.3: Body Area Networks System Model

Table 2.2: In- and On-Body Sensor Applications in BANs

[Ullah et al., 2010]

Application Type	**Sensor Node**
In Body Application	Glucose sensor, Pacemaker, Endoscope Capsule
On-Body Medical Application	ECG, Blood Pressure, Temperature, Blood oxygen
On-Body Non-Medical Application	Music, Social Networking, Forgotten Thing, gesture

BAN applications in medicine: According to the World Health Organization, the global population will reach around 8 billion in 2025 [1], which suggests indirectly that medical applications will become an important issue. In addition, the total healthcare expenditure in the USA is around US$3.5 trillion and is predicted to be more than US$6.5 trillion in 2020 [2]. The use of BANs for medical applications may make it possible to monitor physiological properties, such as body temperature [Drude, 2007, Movassaghi et al., 2014, Wong et al., 2013]. Figure 2.4 shows a wireless medical application of a BAN.

- **Monitoring of human physical data**: Some types of sensors collect physical data from the human body and send the data to healthcare providers for further services. These sensors can be used to monitor human health behaviour [Darwish and Hassanien, 2011].
- **Tracking and monitoring doctors and patient inside a Hospital**: Each sensor has a specific function; for example, a sensor node can monitor the blood pressure and another can monitor body temperature of specific patients. Other sensors carried by healthcare professionals in the hospital may enable them to locate and direct each other to where

[1] http://www.who.int/whr/1998/media_centre/50facts/en/
[2] http://kff.org/medicare/fact-sheet/medicare-spending-and-financing-factsheet/

they are needed [Darwish and Hassanien, 2011].

- **Drug administration in Hospital**: One of the main issues in hospitals is that a patient receives wrong medication. Drug sensors can help prevent or reduce medication errors and avoid associated problems. For example, these sensors can detect and check for sensitivities and allergies to drugs [Darwish and Hassanien, 2011].

Figure 2.4: Wireless Medical Application

BAN applications in sport: Sensors are placed around or on the body to monitor fitness, posture and movement. These sensors can detect the speed and position of the body, and other important vital signs (e.g., pulse rate, temperature) and send them to a medical server [Movassaghi et al., 2014], [Drude, 2007], [Wong et al., 2013]. Figure 2.5 shows a sport device that attaches to the human body and provides data for further processing.

Figure 2.5: Entertainment Device for Monitoring Personal Data

BAN applications in military: The in- or on-body sensors or the environment can be used to monitor vital information about the soldier and to supply key information about the environment, position and soldiers posture and movement [Cavallari et al., 2014]. Figure 2.6 shows a sample of BAN application devices in military.

Figure 2.6: An Antenna Device for Monitoring in Military

2.3 Characteristics of BAN

This section describes the characteristics of BANs such as the technology and communication architecture.

2.3.1 Technologies Used in BAN

Improving BANs is essential to satisfy the wide range of requirements and technology constraints by a particular application, as highlighted in the previous section. The following section discusses the most important requirements.

Embedded operation space in human body: Sensors in BANs are placed in (implantable), on (wearable) or around the body, and they send and receive vital information to and from healthcare professionals. The location and size of these sensors are important to ensuring reliable communication and to saving energy to allow further processing.

Coverage of BAN topology area: The range of topology areas in BANs should not be greater than 3 m for the highest possible number of applications. Most BAN communication uses a star topology with radio scattering, which enables good communication in close range while avoiding adversaries and ensuring secure communication between entities in the BANs.

BAN power consumption: One characteristic of BAN applications is that they enable power consumption in BANs. Many researchers have focused on methods to optimise the lifetime of the battery in BAN sensors, which is a critical issue. An implantable device in or on the body should have a battery of years, so that repeated and potentially harmful surgery is not necessary. Sleep mode in sensors is a common technology that saves power while the sensors are not transmitting data. In addition, ultra-low power is important for wireless networks that

can transmit and receive data through radio or infrared signals [Wang et al., 2015].

BAN antenna technologies: The antenna and radio channel related issues are important since the quality of the signal depends on their characteristics. In addition, the size and design of the antenna in devices are critical issues in existing research on BANs.

BAN data transfer rate: The data rate relies on the application and the transceiver in BANs, and is within the range of 1 kbps to 1 Mbps. This technology is applied to send and receive data through single or multiple links.

BAN sensor node involvement: The number of nodes in BAN technology depends on the type of sensors. For example, less than 6 nodes are used for electrocardiography and less than 12 nodes for glucose monitoring. Increasing the number of nodes can adversely affect BANs and the security within and between them.

2.4 BAN Requirements

To address the growing of requirements for BAN solutions, a number of standards have been developed; one example is IEEE 802.15.6 (Task Group 6 (TG6)), which was developed in 2012 [OASIS, 2005]. Table 2.3 summarises the BAN requirements [Chen et al., 2011].

2.5 BANs Communication Types

This section describes the characteristics of the existing wireless communication technologies used in BANs. These technologies are compared in Table 2.4.

Bluetooth:

- **Bluetooth classic (high speed)**: Bluetooth classic is a form of radio communication that is a short-range standard to support information transfer and some applications, such as voice. A number of devices such as mobile telephones, laptops, MP3 players, Health Device Profile, and others use this standard; there are more than three million such devices in the world[Movassaghi et al., 2012, Patel and Wang, 2010]. The speed of HS Bluetooth

Table 2.3: Requirement for BANs Techniques

[Movassaghi et al., 2012]

Attribute	**Requirements**
In Body Application	Glucose sensor, Pacemaker, Endoscope Capsule
Network size	Less than 64 devices, Max 100
On-Body Non-Medical Application	Music, Social Networking
Data rate	Scalable (less than 1kbps to 10Mbps)
Target life time	Ultra-long
Target frequency	ISM band, (should be low)
Power consumption	Scalable, (from 0 to 0.1 mAh)
Topology	Star, mesh, and tree
Distance	Less than 3 cm or less than 1s after initial setup
Antenna	Omni
Latency	Less than 10 ms
Inter-coexistence	Environment (e.g. ZigBee, Narrowband)
Jitter	less than 50 ms
PER (packet error rate)	Scalable
Duty cycle	Very low for sensor

can supply a data rate of 324 Mbps. HS Bluetooth uses full duplex communication through the use of signals to decrease the overlap between wireless technologies. In addition, this standard shares the 2.4 GHz spectrum with other wireless communication devices [Movassaghi et al., 2012].

- **Bluetooth version 4 (Low Energy) (IEEE 802.15.4 standard)**: Like Bluetooth classic, Bluetooth version 4 is suitable for short-range communication to support information transfer and some applications such as voice. Bluetooth low energy has a star topology and shares the 2.4 GHz spectrum with other wireless communication devices. In addition, it uses the ISM band with a data rate of up to 1 Mbps and supports 79 frequency channels. One of the main advantages of this technology is its low energy consumption, which is ideal for use in BAN devices. This standard enables BAN technology to communicate simply outside the body with a smartphone or other device [Chen et al., 2011].

ZigBee communication: IIEEE 802.15.4/ZigBee is a short-range low data rate radio communication standard for WPANs [Chen et al., 2011]. The rate of data in ZigBee technology is 20 to 250 kbps. Compared with Bluetooth, it provides advantages in power consumption,

latency and lifetime. ZigBee supports mesh, tree, cluster, and star topologies [Movassaghi et al., 2012]. This technology provides good security (128 AEC Encryption) and has elastic networks. Low power consumption, low latency compared with Bluetooth, long lifetime, low frequency, and low data rate enable ZigBee to support BAN applications. Its support of mesh, tree, cluster, and star topologies [Otto et al., 2006], differentiates it from other technologies in BANs. Because of such advantages over other technologies, a number of researchers have focused on this technology [Movassaghi et al., 2014], [Movassaghi et al., 2012].

Ultra-wide band communication (UWB): UWB uses a frequency band of 3.1 to 10.6 GHz. The advantage of UWB is that it causes fewer negative effects on the body, which makes it suitable for health applications; it is also licence free. The free licence and fewer effects on the body make it more suitable than other technologies for use in indoor areas. These qualities of UWB mean it can be used in medical devices in the body and is safe to use in close range communication in a BAN [Xu and Yang, 2008].

Narrowband (NB) communication: NB provides low-power and close-range robust communication at data rates of 121.4 kbps to 971.4 kbps. NB communication is a low RF that is supported by the IEEE 802.15 family of standards such as IEEE 802.15.4 and IEEE 802.15.6 (TG6). The advantages of NB in the TG6 standards are its low power and greater credibility for communication use in the body or within close range of the body. The main problem of NB communication is the inability to support personal area networks in wireless communication. NB communication standards were prepared at the end of 2011 by the IEEE and include the message authentication code (MAC) which supports star topology in BANs. MAC includes three categories to physically layer NB, UWB, and human body communication in BANs, which makes NB efficient in BAN applications. The data rate in NB is 121.4 kbps to 971.4 kbps, which provides a more robust link at lower power in BANs. In addition, NB communication uses DBPSK/DQPSK modulation. DBPSK enables a wide range of data rates. NB communication also supports 39 quiet channels, in conformance with the IEEE 802.15.6 standard, and the maximum payload is very short. As mentioned above, NB communication is suitable for use with close-range devices in BANs [Wong et al., 2013].

Radio frequency identification (RFID): RFID is another BAN technology that includes three components: tagging, an RFID reader, and a host. The principal tasks of the first component in RFID are to keep and send or receive the RFID reader, which is also divided into three

parts: capacity of storage, size, and RF. According to the need for capacity of storage, size, and RF, RFID is deployed in BANs. Read and write tags in RFID enable this technology to be used both at home and in the hospital. Low data rate, low frequency, good security, and simple communication are other advantages of this technology [Movassaghi et al., 2012, Ullah et al., 2010].

ANT communication: ANT technology works with WSNs and aims to support wireless links in BANs. ANT has ultra-low power with a data rate of 1 Mbps, and the design of the technology is simple. In addition, ANT has a low latency and works on the ISM band at 2.4 GHz. ANT can connect with ¡200 device members in BANs, such as those running products, GPS, MP3 players, and heart rate sensors. Additionally, ANT supports the tree, mesh, peer-to-peer, and star topologies. Limited quality of service (QoS), general purpose, and coexistence are some disadvantage of ANT technology in BANs [Chen et al., 2011].

Sensium communication: Sensium radio technology, like ANT, uses ultra-low power, with a data rate of 50 kbps, and works with on-body applications. The star topology of Sensium technology makes it suitable for WSNs. Most of the time, the sensor in Sensium communication is in sleep mode to decrease energy consumption. Sensium allows the health application to monitor and check the state of the body. However, there are some significant disadvantages: it is a proprietary technology that is general in purpose and provides limited quality of service [Ullah et al., 2010].

Rubee communication: Rubee is a form of two-way communication that works in close range with a long-wave signal. Rubee uses magnetic signals and the frequency is very low (around 131 kbps), which sets it apart from other technologies in BANs. The low speed, low data rate, and slow operation are disadvantages of this technology[Chen et al., 2011].

Zarlink communication: Zarlink works through RF communication that it is suitable for transmitting data between medical devices. The sensor in Zarlink has a sleep mode to save power and to increase the lifetime of the battery in IMDs. Zarlink technology is appropriate to use in BAN applications because of the low frequency range (402 to 434 kbps). The need for implantation and the proprietary nature of these devices are disadvantages of this technology in BANs [Patel and Wang, 2010].

Near field communication (NFC): One of the characteristics in NFC technology is the security of communication when the proximity range between the devices and the coverage

area is ¡20 cm. The data rate of NFC technology is in the range of 206 to 424 kbps. In addition, NFC technologies use peer-to-peer topology and ASK modulation. Low data rate and ultra-low power are disadvantages of this technology in BANs [Chen et al., 2011].

2.5.1 Comparison of BAN Communication Technology

According to the description of communication in Section 2.5, Zarlink technology is suitable for use in medical devices because of its low power, low data rate, and reliability; however, the topology of this technology is peer-to-peer. The disadvantages of Zarlink communication are that it is used only for in-body communication (implants). UWB has a low power and high frequency (3.1 to 10.6 GHz), a high data rate, and support in close range around the body, which is appropriate for use in medical devices in BANs. Ultra-low power and high level security are useful features of Rubee technology, but it uses RFID communication. RFID has adverse effects on the human body and sometimes the environment causes reduction in quality, so it is not a suitable technology in BANs.

ZigBee is an effective radio technology for use in BANs because of its low power (lower than Bluetooth). According to this feature, ZigBee is an efficient technology for use in in- or on-body medical devices. Bluetooth classic is another technology that is not a suitable candidate for use in BANs because of its inability to support some devices in BANs. However, Bluetooth low energy is another candidate for use in in- or on-body communication because of its low power, scalability and high rate of data, which are supported in a proximity range and can form an effective interface between two devices within or outside of BANs. High data rate, being supported in close range, high level of security, reliability, low power, quality of service and interference protection, which are supported by IEEE 802.15.6, are reasons for considering NB and UWB technologies as candidates for use in BANs.

Table 2.4 shows a comparison of BAN communication technologies discussed in this section. The advantages and disadvantages of these technologies are listed in Table 2.5.

2.6 BAN Communication Architecture

Communication architecture in BANs is divided into three parts: intra-BAN communication, inter-BAN communication, and beyond-BAN communication, as shown in Figure 2.7.

Table 2.4: Characteristic of BANs Technology

[Movassaghi et al., 2012]

Technology	Frequency	Network Topology	Data Rate	Coverage	Modulation
Bluetooth HS	2.4 GHz -and 5 GHz	Star	3-24 Mbps	<10m	GFSK
Bluetooth LE	2.4 GHz	Star	1 Mbps	<10m	GFSK
ZigBee	2.4 GHz	star, mesh, cluster, tree	20,40,250 Kbps	<10m	QPSK, BPSK(+ASK)
Zarlink	402405 MHz,433-434 MHz	P-to-P	200-800 Kbps	2m	2FSK,4FSK
Narrowband	2.4 2.4835 GHz	Star	1 Mbps	<6m	GMSK
ANT	2.4GHz	Mesh	1 Mbps	<30m	BFSK,FSK
Rubee	131 KHz	P-to-P	10 to 9.6Kbps	<30m	ASK,BPSK
RFID	860 to 960 MHz	P-to-P	10 to 100Kbps	<100m	FSK,PSK,ASK
Near Field Communi-cation	13.56 MHz	P-to-P	106,212,424 Kbps	<20m	ASK
Ultra Wideband	3.1-10.6 GHz	star	110-480Mbps	<10m	OFDM,DSUWB BPSK,QPSK
Sensium	868 MHz,915 MHz	star	50 Kbps	1-5 m	BFSK

Intra-BAN communication: Intra-BAN communication includes communication among sensors on the body and communication between body sensors and external devices such as smartphones and laptops. Intra-body communication is a serious issue in BANs because the attached body sensors have direct communication with BANs. The sensors in BANs monitor vital data from the human body and then transfer the data to the CU or smartphone, as shown in Figure 2.7. The personal data are forwarded from intra-BAN communication to inter-BAN communication for further processing. The lack of battery and energy in the sensors are critical issue to designing energy-efficient protocols [Salehi et al., 2013a,b, Seyedi et al., 2013]. In addition, the sensed physiological data and transfer of critical data between sensors and external

Table 2.5: Advantage and Disadvantage of Communication in BANs

Technology	Advantages	Disadvantages
Bluetooth HS	Low cost, Sufficient data rate, Established Standard, Health device profile specified	Limited security, Limited QoS, Limited scalability, Coexistence with ISM bands, High power
Bluetooth LE	Lower power than Bluetooth classic, Interoperable with Bluetooth	Limited QoS, Limited scalability, Limited design freedom, Coexistence with ISM bands
ZigBee	Lower power than Bluetooth, Smaller memory, Scalable, Healthcare profile specified	Low data rate, Coexistence with ISM bands
Zarlink	Custom designed for implant BANs, Ultra-low power, Medradio compliant	Implants only, Proprietary
Narrowband	Multiple frequency, more channel, high rate and rang/link, scalable	On-body only, limited coverage, support one topology
ANT	Low power, Small size, Simple protocol, Health care device profiles specified	On-body only, Coexistence with ISM bands, Limited throughput, Limited QoS, Proprietary, General Purpose Design
Rubee	Slow technology, Non line of sight communication capability, Ultra-low power, Long battery lifetime	Low data rate, Slow operation
RFID	Non line of sight communication capability, Reusable, Secure reading range, Easy data transmission, Deployment of different frequency band	High Cost, Low data rate, Low operational life of Active RFID, Limitation Coverage of Passive RFID
Near Field Communication	Simple configuration, Easy and Fast communication, Low power	Ultra low range, Low data rate, Low security
Ultra Wideband	High data rate, Low Power, duty cycle, Low electromagnetic radiation, Simple transmitter	Limited Coverage, Complex Receiver, Long signal acquisition time
Sensium	Custom designed for BANs, Ultra-low power	Coexistence with ISM bands, Low data rate, Limited QoS, Proprietary and data rate

devices in the next tier make inter-BAN communication an important issue in BANs in different manner.

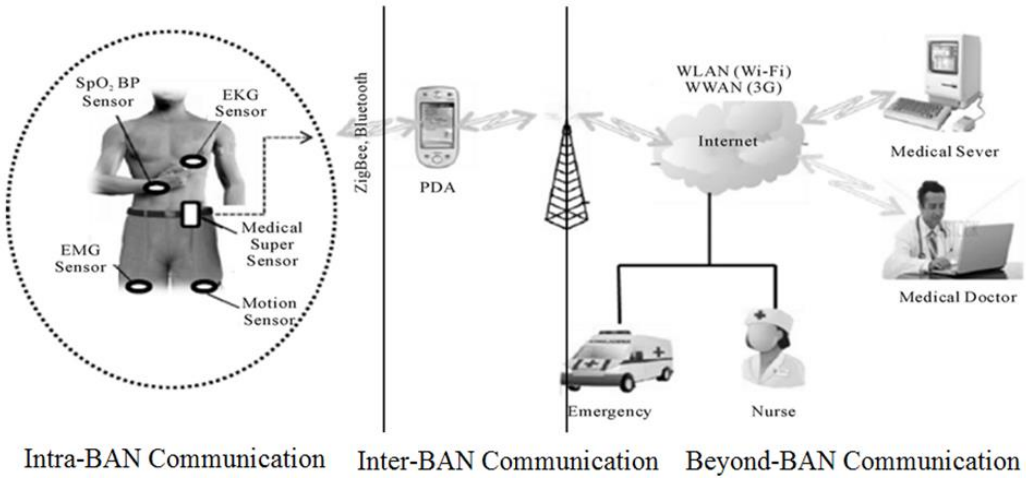

Figure 2.7: Architecture Based on a BAN Communication System
[Kumar and Lee, 2011]

Inter-Body communication: Inter-BAN communication occurs between personal sensors and one or more than one gateway, such as an access point. As shown in Figure 2.7, personal sensors send data to an access point to be forwarded to the medical server via the internet [Movassaghi et al., 2014]. The aim of inter-BAN communication is to connect different networks to each other to allow the easy transfer of personal data. Inter-BAN communication is divided in two subcategories: infrastructure-based architecture, which supplies a huge bandwidth with flexibility, and ad hoc-based architecture, which provides fast deployment in BAN communication [Chen et al., 2011, Seyedi et al., 2013].

- **Infrastructure-based architecture**: Because of space limitations in environments such as homes and hospitals, a number of BANs use infrastructure-based architecture. One of the advantages of infrastructure-based architecture is the security and concentrated management, which highlight the infrastructure base to ad hoc base. Figure 2.8 shows infrastructure-based architecture.

- **Ad-hoc base architecture**: In ad hoc-based architecture, many of the access points are set up to help transfer medical data around the BAN. One of the limitations in BANs is that coverage is limited to 2 m, but the coverage may be increased by using ad hoc-based architecture. Sensors and CUs are two kinds of nodes that exist in ad hoc-based architecture. Sensors and CUs in BANs have the same bandwidth to transmit the data. Because the same interface is shared between CUs and sensors, collisions will accrue. To

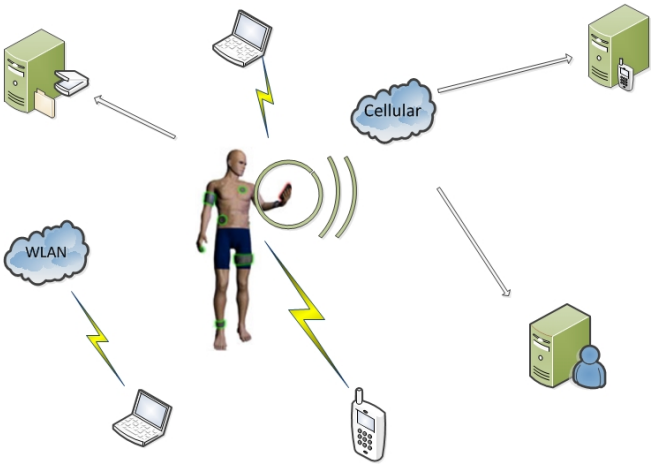

Figure 2.8: Infrastructure Based Mode

avoid this problem in ad hoc-based architecture, ZigBee/IEEE 802.15.4 is used to transfer data between the sensor and CU. Figure 2.9 shows ad hoc-based architecture.

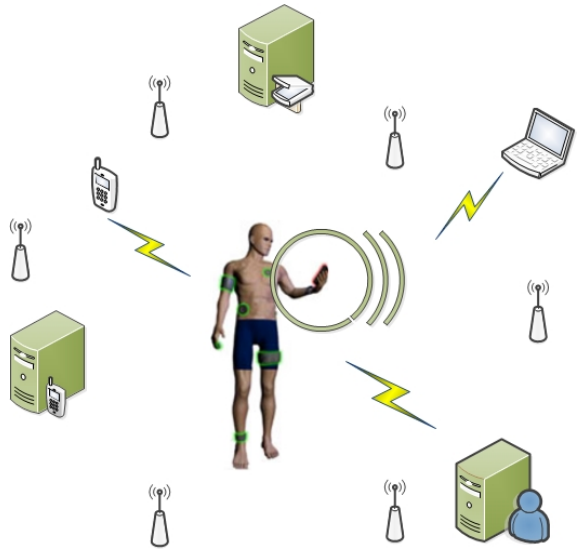

Figure 2.9: Ad-hoc Based Mode Architecture

Beyond-BAN communication: After inter-BAN communication, data must be transmitted to other networks such as a hospital or home. Beyond-BAN communication makes possible healthcare applications that enable physicians to obtain remote access to related data from anywhere. Databases and medical servers in beyond-BAN communication are important because many people can access personal information. Beyond-BAN communication can improve the coverage range and application of healthcare services to connect personal data remotely from any place. The structure of communication in this tier depends on the demand of the users

in a BAN. For example, if the patient has a problem, the system publishes an alarm to alert a physician to monitor the vital data in real time. Beyond-BAN communication is shown in Figure 2.7 [Movassaghi et al., 2014]. Security and privacy of medical data in beyond-BAN are important issues in the current research on BANs.

2.7 Taxonomy of BAN Architecture in Healthcare Environments

Khan et al. [2014] suggested a new framework and routing protocol for monitoring patients in hospital areas (ZK-BAN). They considered two types of communication: point-to-point (p-p), and point-to-multi-point (p-mp) communication. In p-p communication, a CU can transfer data to just one other node, but in p-mp communication, a CU can transfer personal data to more than one node in the same area. The authors used centralised and distributed models in their scenario. In the p-p and p-mp scenarios, the first point is the nearest person, usually a nurse. The second stage is to obtain information about the medical service. Then the health care coordinator for a patient will connect to an access point and transfer critical data to the medical server for further services. In ZK-BAN architecture, the coordinator of patients will send a request to a nurse to obtain new information about another user or health provider when the previous one is unavailable. ZK-BAN offers improved BAN reliability and decreased energy consumption and traffic load related to [Razzaque et al., 2011]. The proposed model is suitable for indoor areas rather than outdoor. The device carried by the nurse operates as a gateway between the patient and physician. If the nurse is unavailable, the patient may obtain the information from other users, which is not safe in same cases. In addition, the ZK-BAN model does not take into consideration the privacy of critical data stored by a coordinator or medical server in the hospital. This proposed model extends a previous model reported by the same authors in [Khan et al., 2012, 2013].

Zhang et al. [2014b] proposed a cluster-based solution for BAN communication in a large-scale network. In this model, the authors assume that each BAN is a cluster, which works like a small network. Wearable sensors send related data to a cluster head (e.g., a smartphone), and the cluster head then transfers the collected data to the medical server via the internet. They presented a network graph to identify which data are sent to other relay nodes. Using graph theory, the authors present a new method to show the data flow in a health environment. This method is called unequal graph partitioning (UGP). UGP can be used to discover clusters

for epidemic control, which demonstrates how sensitive data can be transmitted within BAN communication. The authors also present a framework that includes two steps based on the framework described in [Zhang et al., 2013]. First, they separate the BAN clusters based on population and then apply the crucial algorithm based on graph theory. This framework shows who collects the critical data, and transfers the data to clusters and separates the critical data. They used inter- and intra-clusters for epidemic control within BAN communication to remove the minimal node in clusters. In this way, they can reduce the cost of communication by using inter- and intra-clusters. To ensure privacy of critical data within the BANs communication, they used graph partitioning based on the graph theory model presented by [Zhang et al., 2013].

Razzaque et al. [2011] proposed a quality of service routing protocol to optimise sensor networks. In this model, a coordinator works as a cluster head (CH), and body sensors communicate with the CH. The CH broadcasts hello messages to the body sensors. The data flow between the main nodes (coordinators and base station) in this model increases the traffic of networks, which means that it is unsuitable for BAN scenarios in a large-scale environment. The advantages of the proposed model are a reduction in latency and per packet energy consumption. However, the proposed model could not meet BAN requirements, and security mechanisms are important issues to ensuring secure communication between different parties.

Yuce [2010] suggested a multi-hopping network scenario for WBANs in a hospital environment. To achieve this, author uses a medical implant communication service (MICS) to collect the critical data from body sensors. Then, a wireless medical telemetry service (WMTS) forwards the collected data by MICS to other base stations via the internet. Three scenarios are presented to develop the software and hardware technology. In the first scenario, the coordinator collects critical data from the sensors and forwards them to a local device (e.g. a computer). Then the local device transfers the medical information through the medical server via the internet. The second scenario works in the same way as the first, but there is more than one patient in one room. The medical data are transferred from the patient to the main coordinator installed in the room (home server), and the coordinator forwards the data to the medical server. The third scenario works like the second but on a larger scale. The data are collected from different rooms in the same area and forwarded to the medical server for further services. The second and third scenarios are suitable for applications in an indoor environment. By developing software and hardware tools, the proposed models decrease the delay within the network and increase the number of sensors in the hospital scenario. The proposed model decreases the cost

of healthcare. The weakness of the model described in this paper is the lack of security and privacy of personal data between different stakeholders. These must be considered for ensuring secure communication and protecting the privacy of data from unauthorised users.

2.8 Taxonomy of Data Flow Model in WBAN

Aminian and Naji [2013] proposed a data flow model for use in hospitals. In this scenario, the coordinator collects the personal data and forwards them to the medical server in the hospital area via the internet. The benefits of this method is that it increases the coverage of the network to 10 cm, which increases the life of the networks. However, the results show that the proposed scenarios do not meet the BAN requirements completely. The lack of security and privacy is another disadvantage of this scenario. This scenario is unsuitable for BAN communication in real environments such as indoor and outdoor areas.

Kim and Cho [2009] suggested a network model for data flow and routing protocols within BANs. The authors developed a data flow model to operate for both an individual and a group of people in a small-scale setting. They use p-p, p-mp and mp-p communication flow and transfer related data between different users. Their data flow model is divided into two architectures: personal and public BANs. The first scenario involves a BAN with a coordinator who collects data and forwards them to the medical server via the internet. The public BAN scenario includes a centralised public BAN and uses a distributed model to broadcast data. In this data flow model, each BAN sends a request to another BAN that is near the static coordinator in the environment of the relevant healthcare service. A CU also transmits personal data to another CU carried by patients and the related data are received by the static coordinator. The static coordinator then forwards critical data to the medical server via the internet. In the distributed public BAN, the data flow model is between all BANs. Each BAN is communicated to by the coordinator of another BAN and forwards related data to the medical server without connecting the nearby static coordinator. The proposed model is the first to suggest the use of centralised and distributed communication in BANs. In the proposed model, the data flow is between all personal BANs in environments that are unsuitable for WBAN scenarios. The proposed model does not meet BAN requirements, which is important for a subaquatic data flow model in healthcare areas.

Using key establishment and secure data sent between different stakeholders in homes, nursing homes and hospital environments, [Huang et al., 2009] proposed a data flow model. The proposed healthcare model is based on a hierarchical model of sensors to monitor patients. In this scenario, the nurse, patient and doctors are stakeholders. The doctor can monitor critical data at home or nursing home remotely via the internet. At home scenario, a wearable sensor system (WSS) is attached on the patient's body. The WSS monitors the physiological data and transfers them to a mobile computing device (MCD) carried by a nurse. In addition, the wireless sensor mute (WSM) is installed in different locations within the home and captures different parameters of the environment and communicates with the MCD. The nurse collects and analyses the personal data from the patient and forwards them to the WSM to record in the medical server via the internet. The nursing home scenario is the same as that at home but applies to more than one patient. The nurse collects all personal data from the patients and forwards them to the medical server via the internet. The doctor in the first and second scenarios monitors the critical data remotely from the hospital via the internet. In the third scenario, different users such as patients, nurses, and doctors are in the same building. Each patient has a specific WSS that transfers personal data to the MCD carried by the nurses. Each nurse can collect personal data from one or more patients in the same location. The collected data are then captured from the MCD by the doctor. The doctor can also connect to different MCDs in a home or nursing home remotely via the internet from the hospital to monitor and make better decisions about the patients. The communication between the WSS and MCD is by Bluetooth; ZigBee technology is used between the MCD and WSM.

Haque et al. [2008] suggested a data flow model for indoor areas such as the hospital. The data flow in this scenario is between the patients, a base station and the healthcare service provider. The doctor or nurses send a request to patients via the base station and the collected data are then forwarded to the base station and healthcare provider for further services. Otto et al. [2006] proposed a WBAN scenario and developed software and hardware architecture for health monitoring at home. Using this data flow model, sensors can transmit data to each other as well as to the network coordinators. The network coordinator forwards personal data to the gateway or home server by wireless or cable. The author presented a data flow model that may be applied in indoor areas.

Zhang et al. [2002] proposed a role-based access control (RBAC) delegation framework for critical data to be shared in a medical area between different users (develop RDM2000

framework [Zhang et al., 2001]). According to the particular healthcare scenario, critical information from patients is shared between different parties in the WBAN system. Each user should have specific permission to access the personal information in the network. For example, a doctor can access any data and send a new request to a nurse or other health worker to monitor the patient. The goal of the RBAC is to create a policy whereby all users are granted relevant levels of access to critical information in the networks. It is important to determine how critical data should be shared in a medical environment and between whom and where. A comparison of existing BAN data flow models in healthcare area is depicted in Table 2.6.

Table 2.6: Compression of Existing BAN Data Flow Models

WBANs systems	Sensor	Proposed Scenario	Wireless technology	Security	Privacy	Access Control	RBAC	Frequency Band	other Outcome
[Khan et al., 2014]	ECG, Blood Pressure	Hospital, Home	IEEE 802.15.4 ZigBee	No	No	Yes	No	2.4 GHz	reduced energy consumption
[Khan et al., 2012]	ECG, Blood Pressure	Hospital	IEEE 802.15.4 ZigBee	No	No	No	No	2.4 GHz	reduced energy consumption and traffic load related as well as latency
[Khan et al., 2013]	ECG, Blood Pressure	Hospital, Home	IEEE 802.15.4 ZigBee	No	No	Yes	No	2.4 GHz	reduced energy consumption and traffic load related
[Aminian and Naji, 2013]	Heart rate, Blood pressure	Hospital	IEEE 802.11	No	No	No	No	2.4 GHz	reduced energy consumption and increase coverage ¡10 CM

Table 2.6: Compression of Existing BAN Data Flow Models

WBANs systems	Sensor	Proposed Scenario	Wireless technology	Security	Privacy	Access Control	RBAC	Frequency Band	other Outcome
[Zhang et al., 2014b]	ECG	—	Bluetooth, GSM	No	Yes	Yes	No	2.4 GHz	reduced the cost of communication in BANs
[Razzaque et al., 2011]	EEG, ECG, EMG	Hospital	IEEE 802.15.4	No	No	No	No	—	Reduce latency and energy consumption per packet
[Yuce, 2010]	ECG, EEG, EMG	Hospital	MICS, WMTC, UWB, ZigBe, Wifi	No	No	No	No	433 ISM,3-10GHz, 2.4 GHz	Reduced the delay of network, and reduced the cost of communication
[Kim and Cho, 2009]	EEG, ECG	Hospital	IEEE 802.15.6	No	No	No	No	2.4 GHz	Develop routing

Table 2.6: Compression of Existing BAN Data Flow Models

WBANs systems	Sensor	Proposed Scenario	Wireless technology	Security	Privacy	Access Control	RBAC	Frequency Band	other Outcome
[Huang et al., 2009]	ECG, Blood Pressure	Hospital, Home, Nursing home	802.15.4 ZigBee, Bluetooth	Yes	No	Yes	Yes	2.4 GHz	reduce the average routing latency as well as transmission delay
[Haque et al., 2008]	EEG, ECG	Hospital	IEEE 802.15.4 Zigbee, Wifi	Yes	No	No	No	2.4 GHz	Reduce cost of communication
[Otto et al., 2006]	Heart rate	Home	IEEE 802.15.4 Zigbee, Wifi	No	No	No	No	2.4 GHz	Develop software and hardware
[Zhang et al., 2002]	No sensor	Hospital	——	No	No	Yes	Yes	——	Variety of policy and role

2.9 Security Issues in WBAN

Security issues in WBAN demand effective security methods, such as authentication schemes. As outlined in the literature review of this study, BANs can be used to monitor vital data and how it is transferred from the human body to other places. However, patients also need to be assured of strong security and privacy, as well as safety, to improve the quality of their healthcare service. A number of approaches, such as traditional cryptography, physiological signalling and physical layer security, have been developed in both academia and industry. Each of proposed security models is complex, but these approaches cannot satisfy the security requirements of BANs and also cannot protect the privacy of users in different domains. Better healthcare services require strong security and a reliable and adaptable communication model that can be used to share health information among different parties. Wide deployment of BANs requires the development of efcient solutions to satisfy the security requirements of WBAN. The security threats and requirements, together with their existing security solution in WBAN, are described in the next subsections [Rushanan et al., 2014].

2.9.1 Security Threats

Security and privacy threats in BAN can be classified into the following categories: outsider and insider attacks. In an outsider attack, the attacker is not an authorized participant of the sensor network. To prevent outsider attacker regarding access to the data, authentication and encryption methods are required in sensor networks. The intruder node can only be used to launch passive attacks, like passive eavesdropping, denial of service attacks, jamming, and replay attacks. In addition, an insider attack is able to obtain the key material of nodes and modify or forge node messages. Unauthorized access, false data injection, selective reporting and modification are kinds of active attack in sensor networks. Regarding insider and outsider attack in WBAN, security threats from device compromise, as well as from network dynamic, are found in the literature.

Threats from devices that compromise: The sensor nodes in a WBAN are subjected to compromise, as they are usually easy to capture and not tamper-proof. If a whole piece of data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of data[Rushanan et al., 2014].

Threats from network dynamics: The WBAN is highly dynamic in nature. Due to accidental failure or malicious activities, nodes may join or leave the network frequently. Nodes may also die out due to lack of power. Attackers may easily place faked sensors in order to masquerade authentic ones, and can take away legitimate nodes deliberately. The patient-related data, if not well kept in more than one node, can be lost easily due to the network dynamics. Also, false data can be injected or treated as legitimate, due to lack of authentication[Rushanan et al., 2014].

2.9.2 Security Requirements

The communication of critical data in a Wireless Body Area Network has to comply with the following security requirements:

Confidentiality: Patient-related data should be kept confidential during storage periods. Most particularly, its confidentiality should be robust against node compromise and user collusion.

Integrity and Authentication: The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.

Availability: The patient-related data should be accessible even under denial-of-service (DoS) attacks and also, data freshness is necessary to detect replayed packets.

Non-repudiation: Prevents the denial of previous queries submitted by the user in WBAN network. That is, if the user has submitted a query message to the WBAN, it cannot deny its action.

In addition, the problems associated with security is increasing nowadays. The privacy of communication through the Internet may be especially at risk of being attacked in a number of ways. On-line collecting, transmitting, and processing of personal data make up a severe threat to privacy. Once the utilization of Internet-based services is concerned, the lack of privacy in network communication is the main conversation for the public. This problem is far more significant in a modern medical environment, as healthcare networks are implemented and developed. According to common standards, the network linked with general practitioners, hospitals, and social centres at a national or international scale. While suffering the risk of leaking privacy data, such networks can reduce the costs and improve the effectiveness of the

healthcare system. Security solutions in BAN must provide confidentiality, integrity, availability (CIA), non- repudiation and access control policy for the data, while permitting exclusive access to doctors, nurses, and any healthcare services provider [Lee et al., 2014].

2.9.3 Security Solutions

The security issue is one of the most important aspects in BAN applications, especially in healthcare environments, because sensitive health data must be protected from unauthorized users; such unauthorized users can be dangerous to a user's life.

The existing security techniques and protocols used in WSNs and MANET are not suitable solutions to be used in BAN because of the different characteristics and network architecture between WSN, MANET and BAN. These characteristics include the number of sensors attached on or in a body, range of communication, size, and power that is typically quite limited [Ahmad et al., 2015]. As a result, when designing security protocols for WBANs, these characteristics should be taken into account in order to dene optimized solutions with respect to the available resources in this specic environment. In addition, several security models have been proposed in protecting sensitive data between sensor networks such as Dife-Hellman (DH), Elliptic Curve DifeHellman (ECDH), physiological signal characteristics and wireless channels. Due to several reasons, such as high communication and computation and also using additional hardware, we need to focus to overcome these problems to meet the security requirements in BAN[He et al., 2016, Zhao et al., 2016].

Summarizing the above and the associated literature, it is clear that the access control policy method, which is more capable than other techniques of achieving all the security requirements in WBAN from a healthcare point of view, is missing in existing studies. Since it is important to allow on-demand access policy adaptations during healthcare, a future direction is to design more flexible, cryptographic enforced, and access control policy model for WBANs.

2.10 Policy Models Based on Healthcare Environments

The last section of this chapter describes the existing data flow models in healthcare areas. This section starts with a review of the literature about the third objective of this research project, as outlined in the preceding chapter.

Much research has focused on the use of RBAC in healthcare models to enable authorization for different users based on their roles and responsibilities [Ferreira et al., 2011, Shin et al., 2015, Zhang et al., 2001, 2002]. Zhang et al.[Zhang et al., 2002] proposed a RBAC delegation framework for critical data to be shared between different users in a medical area. According to the particular healthcare scenario, critical information from patients is shared between different parties in the WBAN system. Each user has specific permission to access the personal information in the network according to their duties. The goal of the model based on RBAC is to create policies whereby all users are granted relevant levels of access to critical information in the networks. The authors developed the RBAC model based on different policies. Their policy model is based on the medical environment: how critical data should be shared between roles and where and who can access these data according to their attributes.

A number of research has also focused on policy models with respect to environment management [Ardagna et al., 2008, Bettini, 2002, Ni et al., 2010, Toninelli et al., 2006]. The goal of this type of model is based on the behaviour of environments. In this model, the policies are defined based on the environmental requirements to take particular action. The advantage of the model developed is that it can set a new level of access for users as needed. However, a decision about granting new access based on this model can take a long time, which makes this model unsuitable for critical functions in healthcare areas [Bettini, 2002]. Ardagana et al. [Ardagna et al., 2008] developed a policy model that included different groups, called Policy Space. The goal of this model is to provide access in critical situations In this model, the group policies can be changed very easily for each user and during an emergency. However, the disadvantage of this model is that the unauthorized user may be able to access sensitive data in an emergency situation. This model needs some subpolicies for individual cases to satisfy the privacy requirements.

Lorch et al [Lorch and Kafura, 2002] developed a model to grant access to users. The model defines policies according to the users activity in their domain. The users can access sensitive data according to their attributes. The results and framework presented in this model show that new access and access to other users can be granted without sending requests to administration. The disadvantage of this model is that the privacy of users is not considered in different environments because users may be able to access to resources without any authority control.

To address the limitations of the model developed by [Lorch and Kafura, 2002], Nazare et al [Nazareth and Smith, 2004] defined attribute release and acceptance policies, which they called ARP and AAP. Developed policy model in this research model is defined regard to users attributes. To provide privacy, ARP is applied to users and AAP is defined for resources and different situations in the domains. The drawback of the model is that the policies defined for users cannot be changed easily if there is a change in the sublocation in the same place. For example, a doctor can access data about patient A in the surgery department for further services. However, that doctor may need to send new request to access to the same patient's data from other departments in the same hospital. Morchon and Wehrle [Garcia-Morchon and Wehrle, 2010b] developed a policy model based on healthcare environments. Their model is based on a quick reaction to users in emergency situations. However, the model does not address the privacy of sensitive data, although a new level of access is provided for users. Thus, the model is not suitable for emergency situations because new users need more interaction with other users in same location. policy models based on healthcare environments are unlike other security solutions in sensor networks. In policy model is important who can have what type of access to which objects owned by whom at which location and what time. In addition to this complexity, the absence of a trusted centralized authority forms a major technical challenge in developing security protocols that meet the WBAN eHealth security requirements.

2.11 Summary

A BAN comprises different types of medical sensors placed in, on or around the human body to collect critical data from the body. The data collected are transferred to a medical server using wired or wireless mechanisms. In a wired system, each sensor is connected to an external medical device. However, using wireless technologies, the sensors can connect to the coordinator (CU) that is near the BAN. The CU works as a gateway between the sensor and other networks around the BAN to collect related data from body sensors. BANs can communicate with each other in the same location and, if needed, in other locations. Each BAN uses a different wireless technology with a different frequency to transfer data from the inside to outside areas as well as in the reverse direction. The literature indicates that a number of elements (e.g., latency, delay, less energy, low rate data and short-range communication) have different impacts on BAN communication within and between other BANs.

It is important to consider how the data flows between different users in a variety of areas according to the responsibilities, rules, policies and duties. The data flow models and BAN architecture analysed here focus on how the data flow between different users and who has access to medical data according to the roles and policies. The privacy of patients data is another important issue to be considered during the communication process within and between BANs. In a BAN scenario, it is important to identify who may have access to patient data and how the data may be accessed; for example, using a smartphone or another point in the network, such as a medical server.

To address these challenges, unique data flow models are needed that can extend to both indoor and outdoor scenarios. Many studies have focused on mobile computing and communication to permit patients to move freely and to be monitored at any location at any time. However, these models focus on individual patient monitoring in indoor environments, and healthcare and remote healthcare monitoring of small and large groups in indoor and outdoor environments have not been addressed. In addition, there is no access control policy model based on indoor and outdoor healthcare areas to develop new technologies to provide pre-existing relationships between the subject, object, resources and their environmental attributes as the subject moves freely. Solutions to these challenges require the development of appropriate policy models based on the data flow model developed in this study.

Chapter 3 discusses healthcare scenarios with regard to indoor and outdoor environments and various parties in real-life situations as a step toward preparing a fundamental plan for next step. The scenarios presented examine the requirements and characteristics needed to support and model the relationships between the various parties in a health system and show how input health information can be transmitted to output with a high level of detail. Building on these requirements, characteristics and data flow models, an access control policy is modelled in Chapter 4. Access control policy models can provide different policies based on each environment and the parties, which may have different relationships with each other. These policies can filter the permission before granting access to users. This can prevent conflict of permission when assigning access to users in the same location.

Chapter 3

Data Flow Models Developed for Wireless Body Area Networks

3.1 Overview

This chapter focuses on the data flow model in medical environments and describes the architecture and data flow model developed for BAN communication within and between healthcare environments. Sequence diagrams are presented that use Unified Modelling Language (UML) 2.0 to illustrate and investigate the accuracy of the data flow models developed in inter- and intra-BAN communication. Petri Nets (PNs) are used to analyze and validate the models. This analysis allows one to monitor health information as input and the result as output. It is helpful to examine the design carefully and critically during modelling and testing. Variety of stakeholders in on-body BAN application depicted in Figure 3.1.

As shown in Figure 3.1, medical applications in on-body domains are used to monitor healthcare information in different areas. Considering the nature and characteristics of medical applications in different environments, we have identified two types of BAN communication scenarios: indoor monitoring and outdoor monitoring. In Figure 3.2, the general architecture is presented to determine the type of BAN applications in on-body domains. Recently, many researchers have focused on healthcare systems and applications that can help to improve the quality of health services and to ultimately improve patient safety and quality of life.

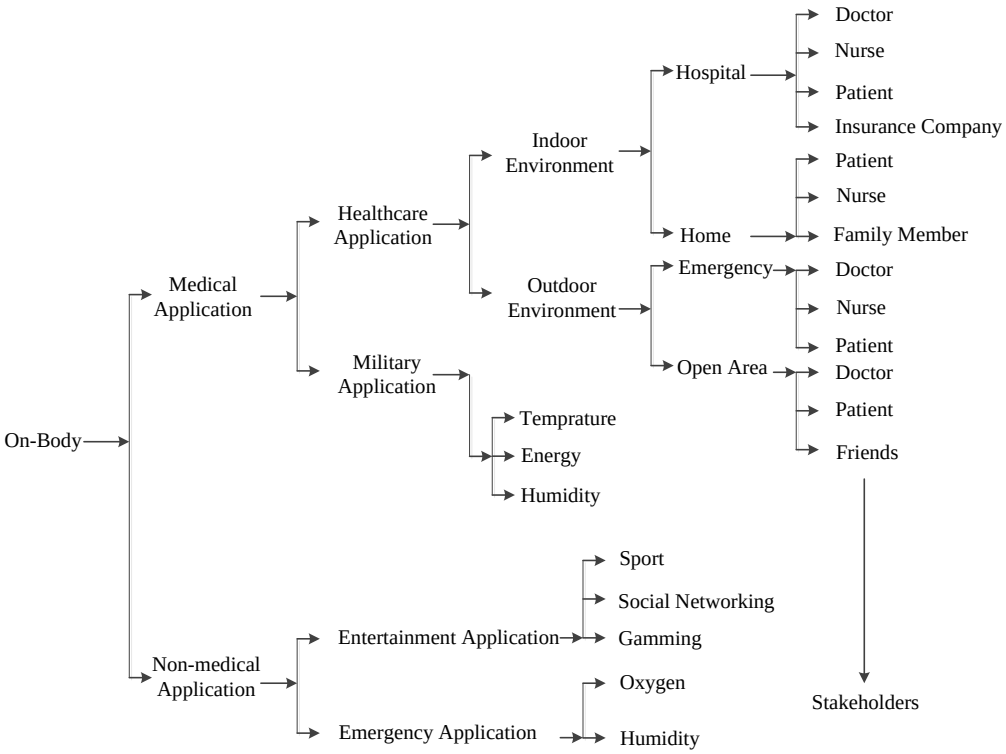

Figure 3.1: Stakeholders On-Body BAN Application

Figure 3.3 shows the general indoor and outdoor scenarios involving multiple stakeholders.

3.2 Data Flow Models

This section describes the model developed and how the data flows between different stakeholders within and between the BAN systems in small- and large-scale networks. Based on open networks, different scenarios are presented, such as open areas, emergency vehicles, homes, and hospitals.

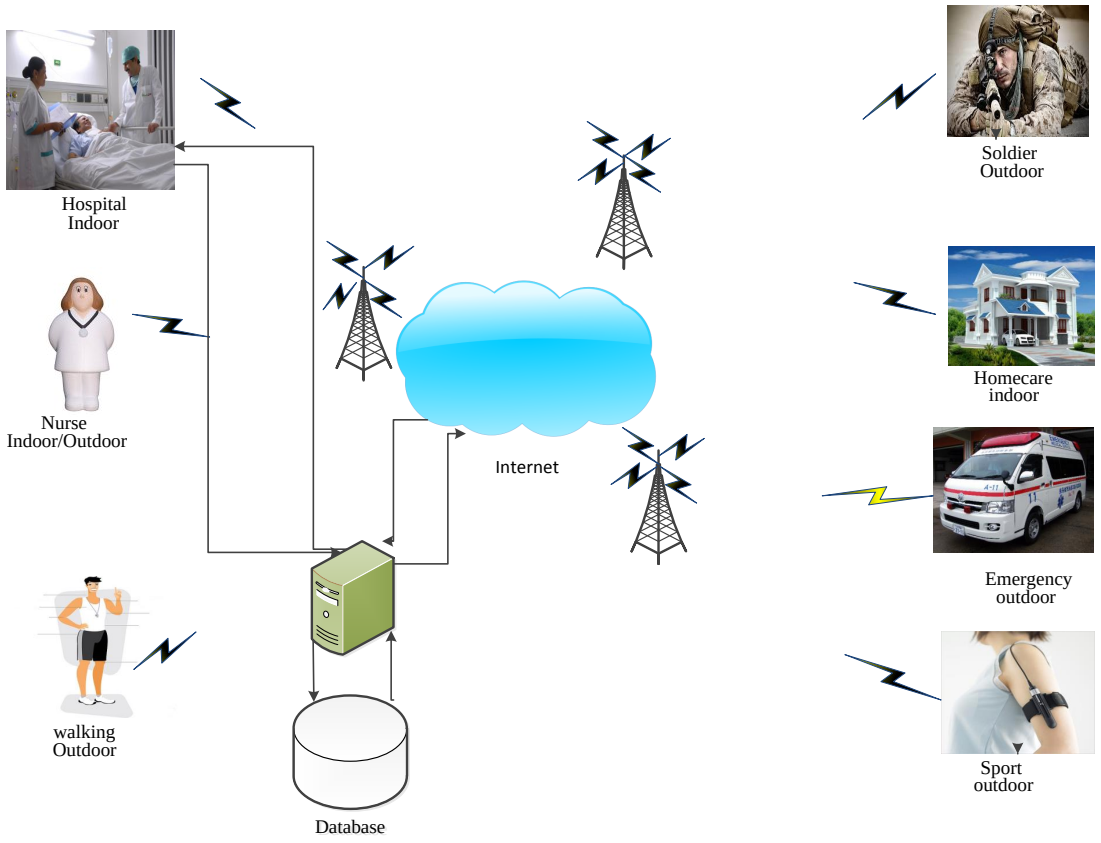

Figure 3.2: Indoor and Outdoor BAN Application in Medical Domain

3.2.1 Data Flow in Healthcare Scenarios

In this section, data flow models are proposed for open area, home, hospital and emergency scenarios as general model depicted in Figure 3.3.

- **Open area data flow model**

This section describes the data flow between different parties, such as patients, doctors and medical servers, in an open area. Figure 3.4 illustrates the data flow model for an open area scenario within BANs and any healthcare service. In this scenario, the physician can publish a pain alarm from the hospital through the control unit (CU) to monitor the patient from outside the hospital. The doctor may also publish a request to the medical server or connect remotely to the CU via the internet. The data are transmitted to the nearest base station (BS) and then to the other node. The doctor can publish a pain alarm from outside the hospital via the internet using

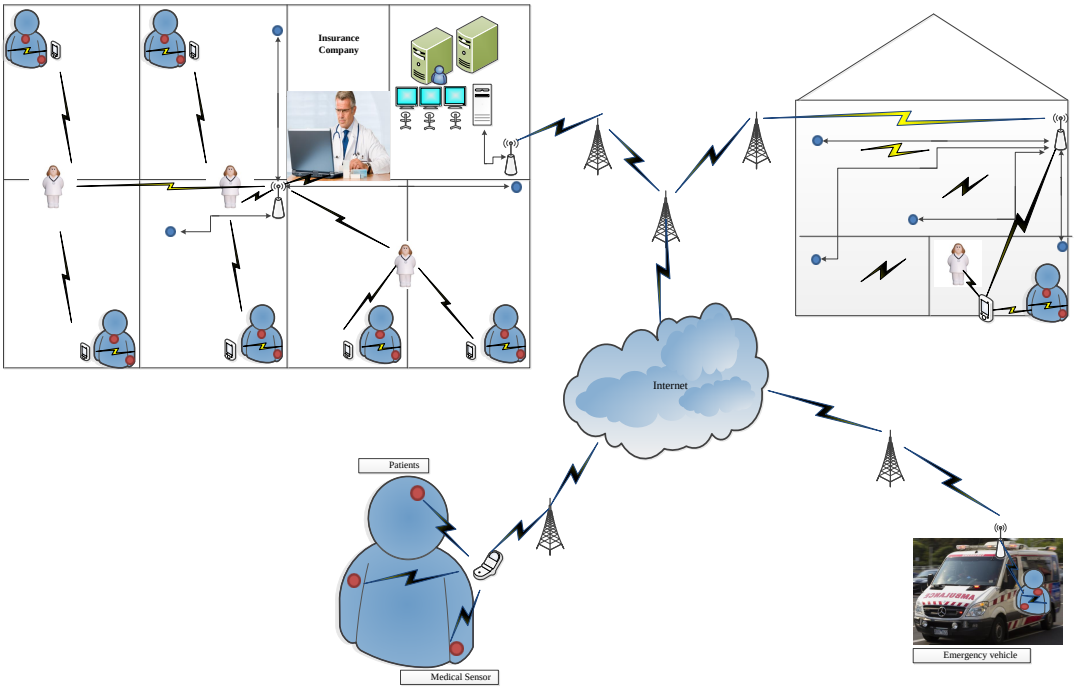

Figure 3.3: Hospital, Home, Emergency, and Open Area Scenarios for Medical Application within and Between the BANs

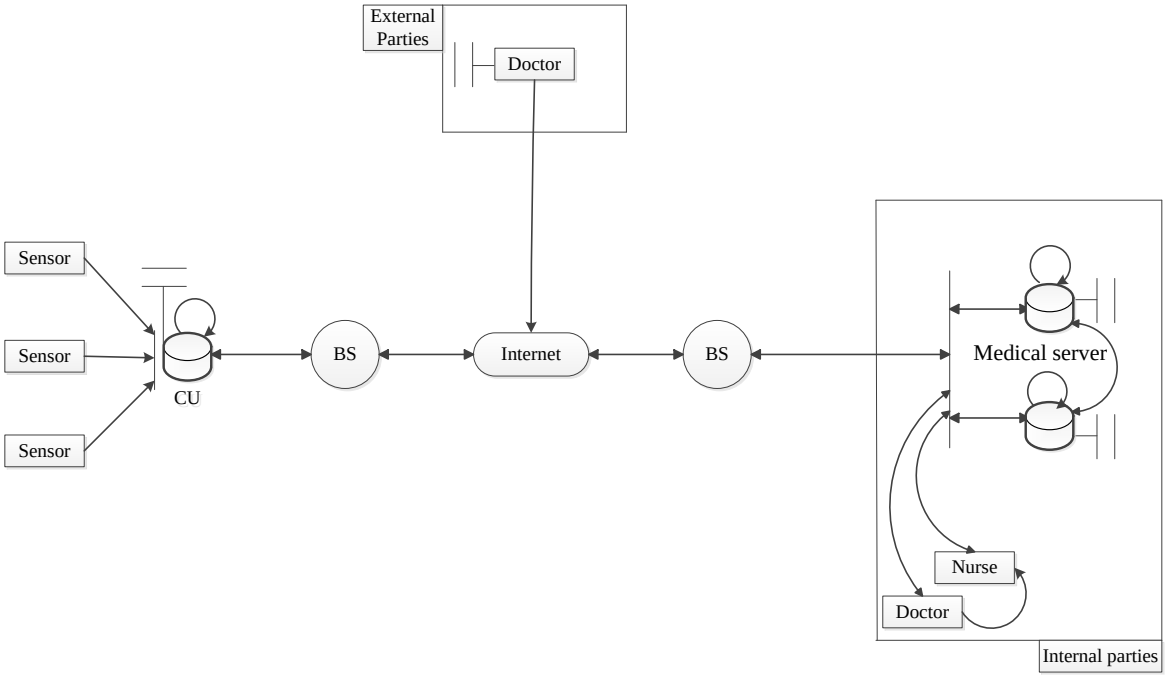

Figure 3.4: Open Are Data Flow Model

4G/3G or GPRS technology. The requested pain alarms from the physicians are received by the CU carried by the patient. The CU uses wireless technology such as 4G/3G or GPRS. The CU responds to the doctor or nurse if the requested data are fresh and available in the database; otherwise, the CU forwards a request to the body sensors, which collect physiological data and transfer that data to the CU. The CU works as a database while receiving new data and transfers the data according to the request published by a different physician. The collected data are transmitted to the medical database via the internet by a different relay BS. The physician can access the medical data through different access levels. The accuracy of the data flow model in an open area scenario is presented in a sequence diagram in Figure 3.5.

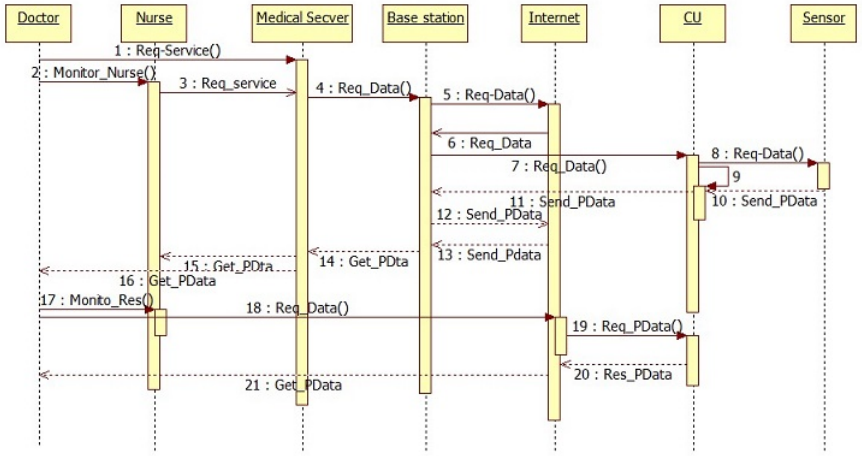

Figure 3.5: UML Sequence Diagram for Open Area Model

- **Emergency data flow model**

This section presents the data flow between different parties in an emergency scenario. Figure 3.6 shows the data flow model for an emergency scenario.

In this model, the doctor or nurses monitor the patient by connecting to the CU via a wired or wireless system. After the initial analysis, the data are forwarded to the hospital from the telemedical device (TMD) by a different technology such as 4G/3G or GPRS via the internet. The data are recorded in the emergency vehicle and the medical server in the hospital for further services. In addition, the doctor can connect to the CU remotely from any place to continue to monitor the patient. The accuracy of the data flow model is presented in a sequence diagram in Figure 3.7.

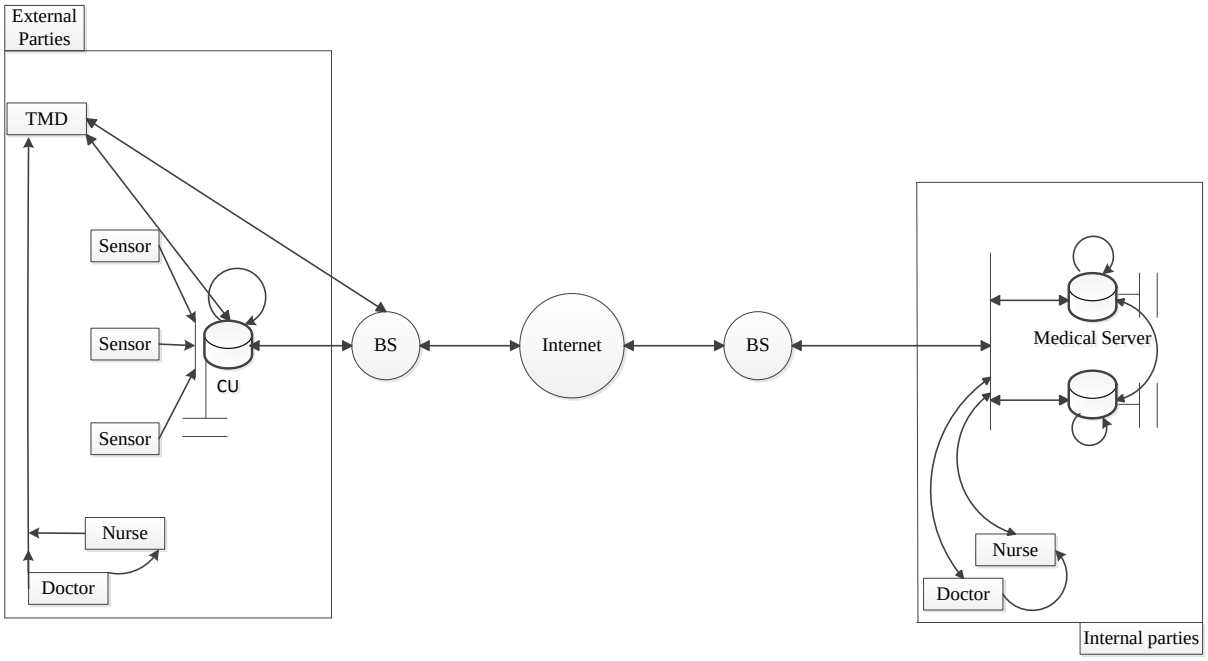

Figure 3.6: Emergency Data Flow Model

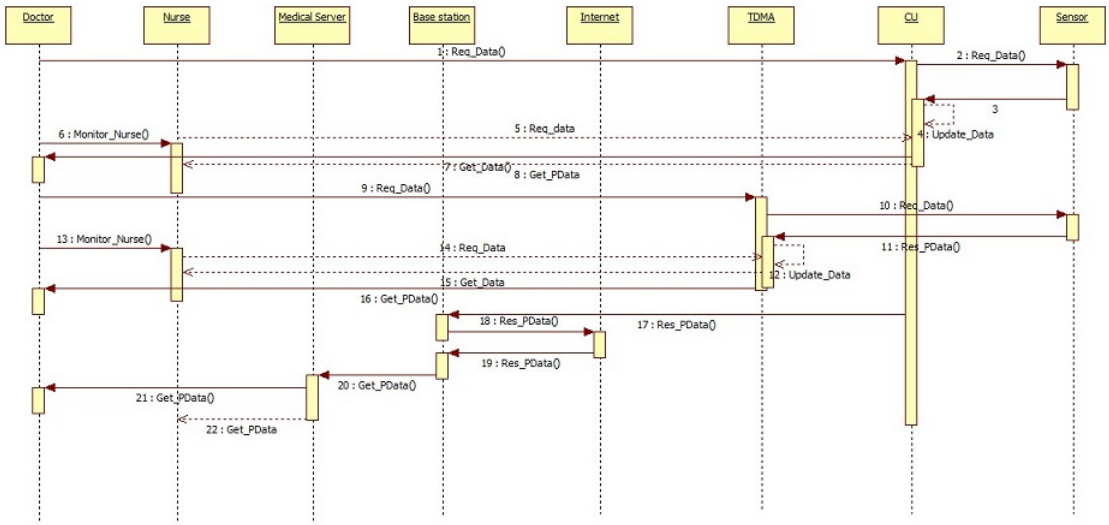

Figure 3.7: UML Sequence Diagram for Emergency Model

- **Home data flow model**

This section describes data flow between different parties from home areas (e.g., communication between the patient and environmental sensors at home and the medical server in the hospital or any physician). Figure 3.8 illustrates the data flow model for different stakeholders

in the home scenario. In this model, the data flow between different parties between the home

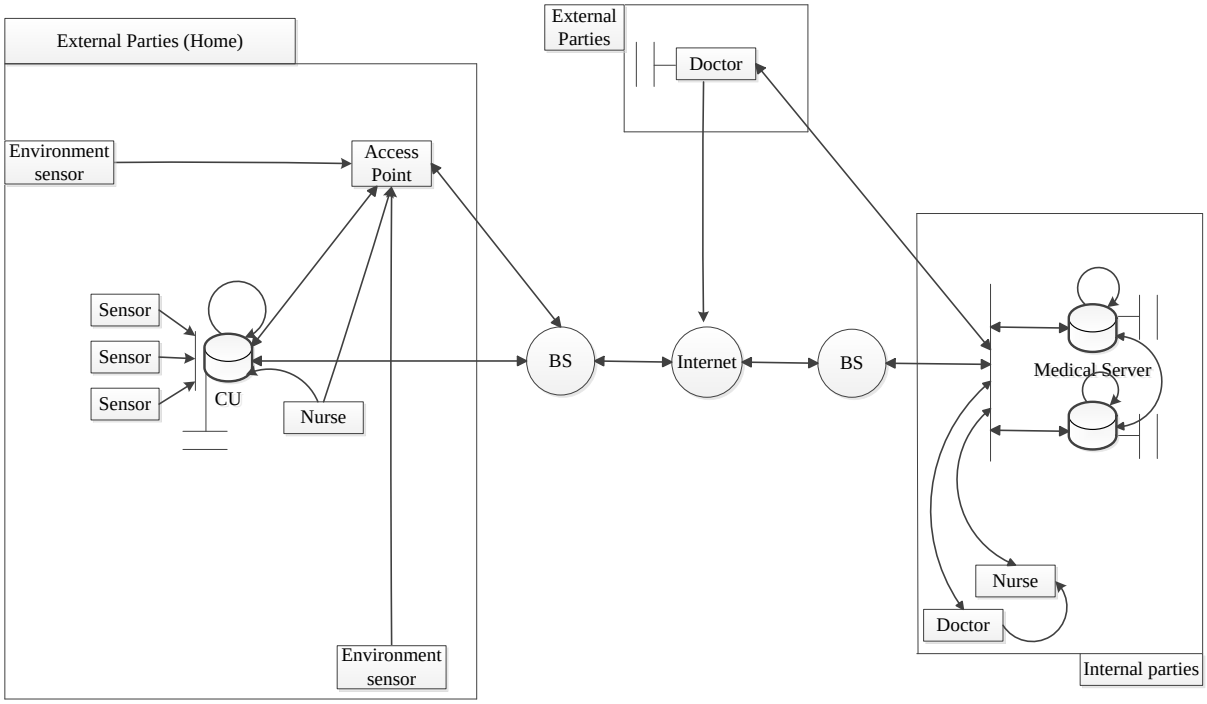

Figure 3.8: Home Data Flow Model

and healthcare provider services. The doctor checks the patient's state initially and publishes an instruction, such as the need to monitor vital data. This event is recorded at medical server in the hospital. The doctor can also publish a new instruction to monitor the personal data by forwarding the requested data via the internet. The requested data are forwarded to the nearest relay base station and finally received by the home server. The home server receives the data by a different mechanism, such as ADSL, and transmits it to the access point. Then the access point shares the data in the home environment. The CU receives and records the data shared through the access point. The CU will then send a request to the body sensors attached to the patient instructing the sensors to collect the relevant vital data and forward them to the home server via an access point. The nurse has lower-level access to medical data at home. For example, a nurse can change a patient's prescription based on the recorded data.

Environmental sensors collect environment data. Environmental sensors and CU then transfer the data to the medical server via the internet. The physician can analyse the monitored data in the hospital and change the event if necessary. The data in any medical database such as a CU, home server, or medical server in the hospital, are recorded to be used by a healthcare

service provider.

The policy of the data flow model allows different users to have different privileges to access medical data. The doctor has full permission to access medical data in a medical database directly or remotely. A nurse can access the data stored in a CU as well as other data recorded in the medical database in the hospital, but at a lower access level than the doctor. Insurance companies have limited access to the medical data in the hospital. The insurance company can access general information such as a patient's name, age, and other common types of data about the patient. Family members can access medical data recorded on the CU if permission is granted by a doctor or the patient. Using this model, data between different stakeholders can flow to other relay nodes through the same mechanism and technology. A sequence diagram to describe the accuracy of the data flow model in a home scenario is presented in Figure 3.9.

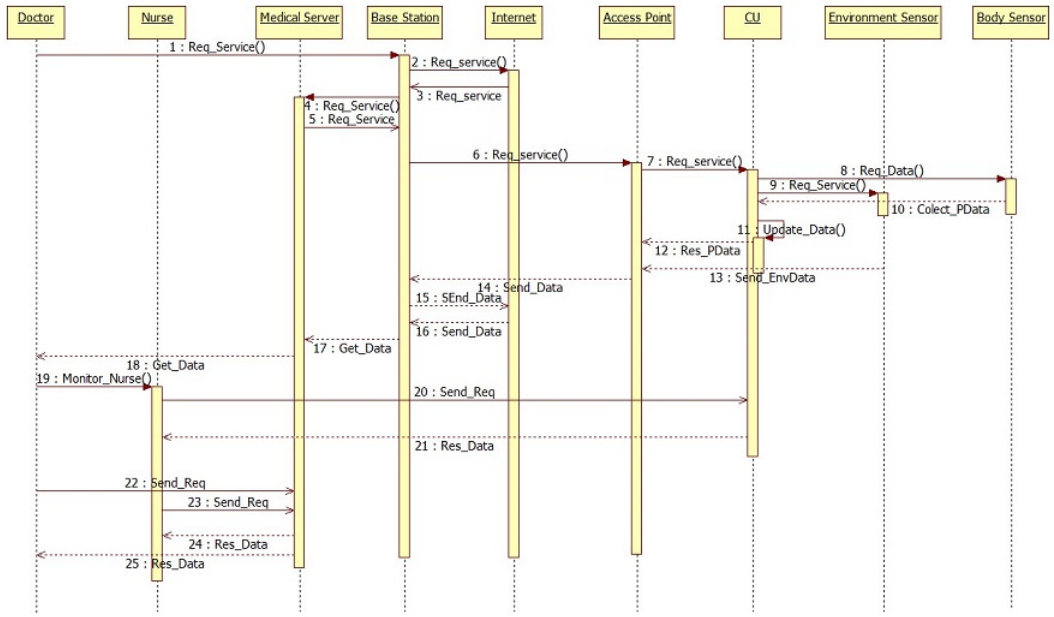

Figure 3.9: UML Sequence Diagram for Home Model

- **Hospital data flow model**

This section discusses data flow between different parties in a hospital scenario. Figure 3.10 shows the data flow model for a hospital scenario.

This data flow model is a more complex scenario compared with the other models. This scenario includes different users, such as the patient, doctor, nurse and insurance company,

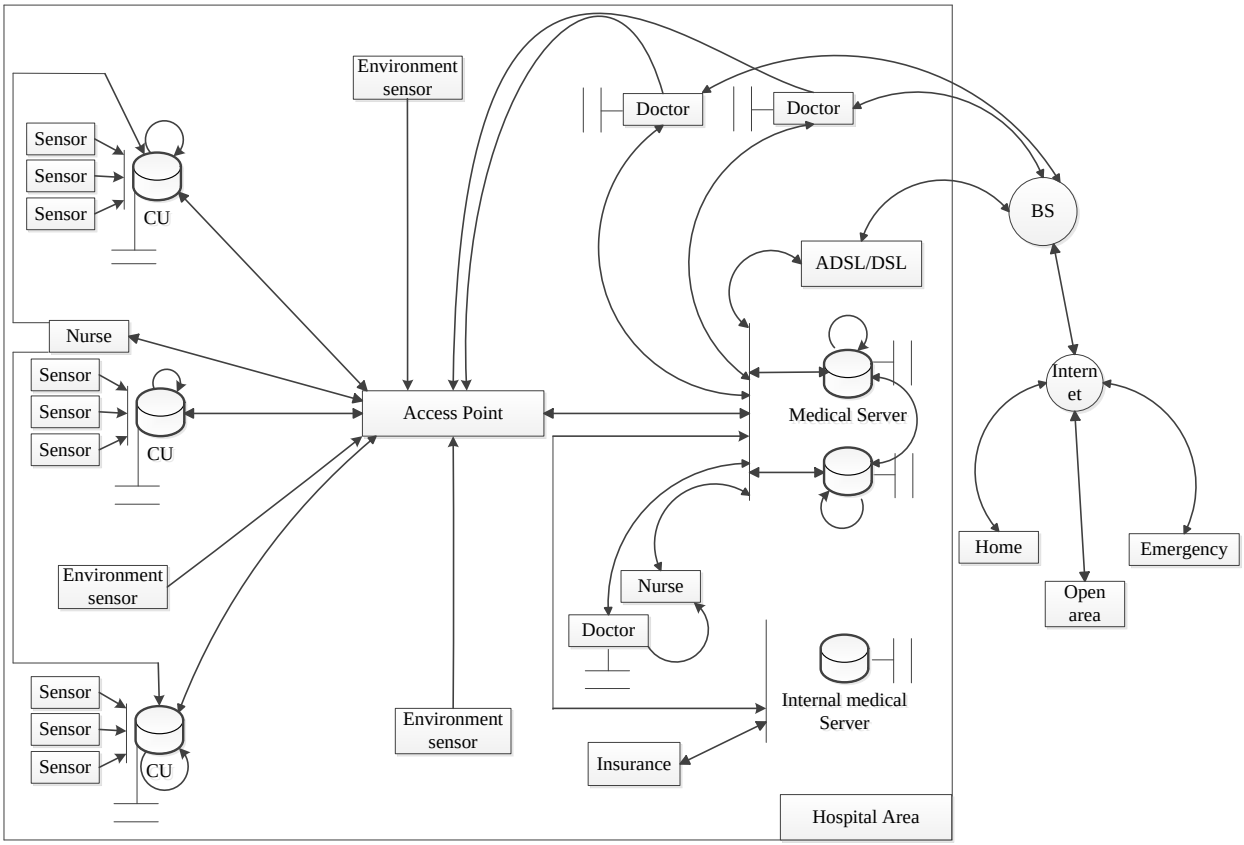

Figure 3.10: Data Flow Model in Hospital

which can communicate with each other within the same location using different technology, access levels, responsibilities and levels of privilege. It is assumed that several patients are in the hospital. Each patient has a personal control unit that sends and receives personal data to the access point via wireless technology shared in the hospital. Based on the different roles and policies introduced, the patient, doctor, nurse and insurance company each have different privilege levels and instructions about who has access to the medical data. For example, the doctor can publish a new event from inside or outside the hospital, but the nurse can access the medical data only at the hospital. The event is then forwarded to access points where it can be shared within the hospital environment. After that, the access point transfers data to the patient via wireless, where it is received by the CU. The CU sends a request to the body sensors to obtain new physiological data from the patient. The CU collects personal data from the body sensors, stores the data in the database, and forwards the requested data to the medical server. The CU then forwards the requested data into the medical server via the access

point. The medical server records the personal data and then forwards them to the doctor, nurse and an internal server to be used by the insurance company. The environmental sensors installed in different locations in the hospital record and monitor the state of the hospital. These environmental sensor transfer the recorded data to the medical server for further services.

The doctor has full permission but the nurses may have more restricted permission to access the medical data in real time. The insurance company can access the internal medical server with certain access limitations. For example, it can access general data such as the name and address of the patient, but the insurance company cannot transfer any data about the patient or request information directly from the medical server. The medical data, when forwarded from an open area, emergency or home scenario, are recorded in the medical server and are updated according to defined instructions. Data can be transferred to other scenarios. The next section analyses and discusses the proposed data flow models in terms of communication, access levels and other requirements. To describe the accuracy of the data flow model in the case of the hospital scenario, a sequence diagram is presented in Figure 3.11.

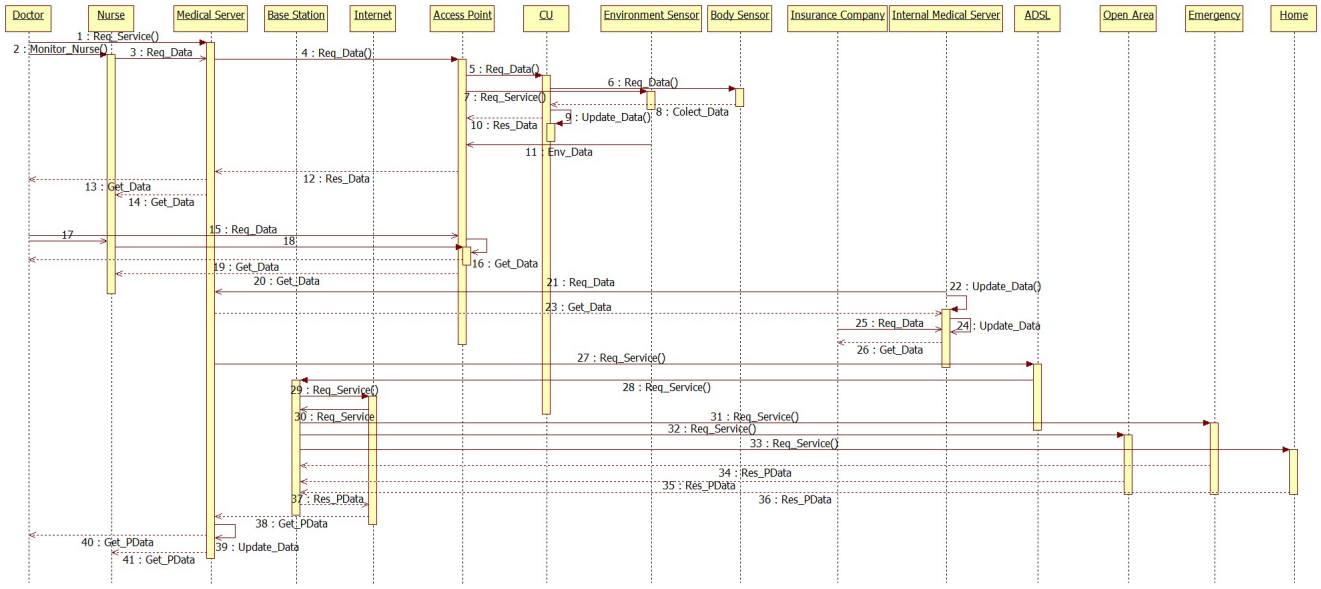

Figure 3.11: UML Sequence Diagram for Hospital Model

The entire data flow model is shown in Figure 3.12. In each scenario, the data are forwarded via the internet to the hospital to record the medical data in the hospital for further services. Doctors have access to the medical server or any database such as the CU from inside and outside the hospital. The accuracy of the model is described in the sequence diagram shown in Figure 3.13.

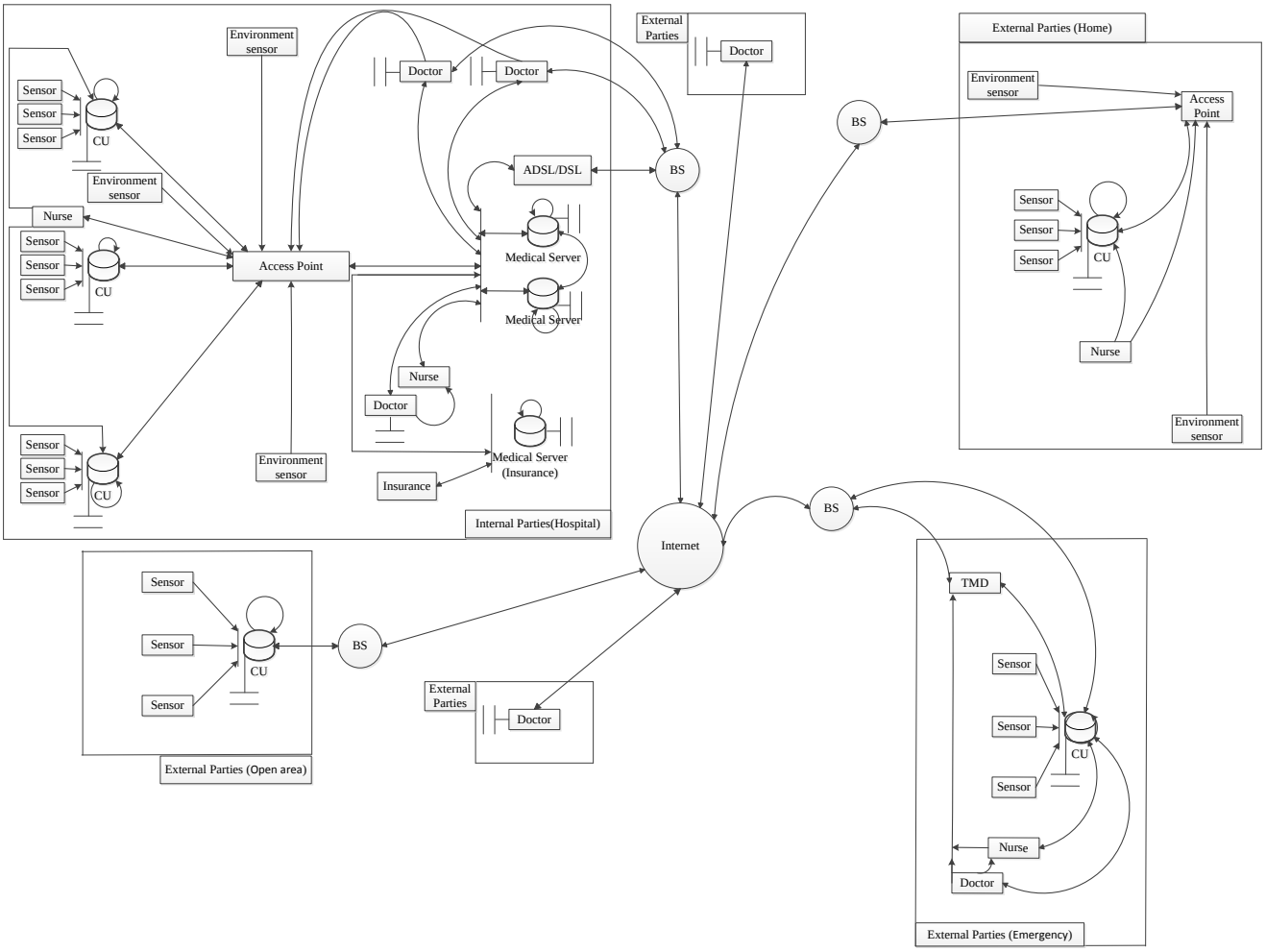

Figure 3.12: Proposed Data Flow Model Within and Between the BANs

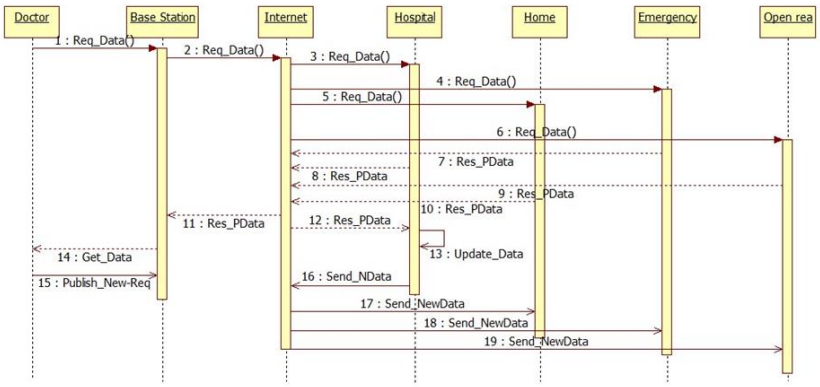

Figure 3.13: UML Sequence Diagram for Backbone Model

- **Analysis of sequence diagrams**

In this section, the sequence diagrams are described using UML 2.0 to illustrate the functions of the data flow models developed. The purpose of this section is to show how the data are transferred and shared between stakeholders with different access levels in indoor and outdoor environments. This information is useful for testing and critically reviewing the proposed model.

Open area model: Figure 3.5 presents a sequence diagram for the open area model, in which the physician sends a request for service (REQS) to the next hop (medical server). The medical server forwards the REQS to the multi-hop to be received by the coordinator (e.g., smartphone). The REQS is redirected by the CU to the body sensor and collects the relevant data and response service (RESS), which includes the medical information. The doctor has permission to remotely connect to the CU, as shown in Figure 3.5. The CU updates the existing database while collecting the data from the body sensor or medical server.

Emergency area model: Figure 3.7 presents a sequence diagram for an emergency scenario, in which the doctor and nurse connect to the CU or TMD. A TMD is a medical device that obtains images and collects data during a patient encounter. The TMD or CU sends a REQS to the sensor, the critical data are collected, and the existing databases are updated. The collected data are forwarded to the doctor, nurse and medical server to record and analyse the information.

Home model: Figure 3.9 shows the sequence diagram for a home scenario. The doctor connects to a different home database from any location and sends and receives information. The home server collects data from the CU and environmental data by the access point and forwards them to the medical server. The doctor also sends an REQS to the medical server to monitor personal data recorded in the medical server.

Hospital model: Figure 3.11 presents the hospital sequence diagram that shows the complete sequence diagram, including the number of BANs in the hospital and the relationships between the hospital and open areas, emergency situations, the home, and doctors. One of the main issues in the hospital area is adding and removing different patients (i.e., personal BANs) by different technology and service requests. he CUs carried by the patients need to connect to the networks. New patients sign up the system when they are admitted to the hospital for the first time. To do this, the CU sends an REQS to an access point. An access point in the

hospital works like a static wireless coordinator to register new CUs into the network using unique information such as the patient's identification number (ID) or BAN. Then, a doctor or nurse sends an REQS to a medical server or access point. The access point checks the REQS and shares it, and it is received by a specific CU. The CU collects data from the body sensors and indirectly through RESS to the access point using the unique ID. The access point checks the ID on the existing list and forwards the data to the medical server, doctor and nurse, who can access the data according to their access level. The database in the CU, the access point and the medical server are updated to respond to the physician's needs in a short time. As shown in the sequence diagram, in this scenario, a personal coordinator cannot access or connect to other personal coordinator's area to send or receive data. The REQS is forwarded to the emergency location, home and open area for monitoring by the physician in hospital via the internet, and the RESS data are redirected to the medical server for further services. Figure 3.13 represents a sequence diagram of the backbone communication between doctors, hospital, home, emergency and open areas described above.

- **Analysis of the Developed Data Flow Model Based on Petri Nets**

This section discusses data flow models in hospital, home, emergency and open areas designed using PN software. PN software is an appropriate model for verification and validation modelling language for the distribution system. PNs permit formal analysis and creates a graphical shape that is a logical model that helps to understand the system model using basic knowledge. A PN is a flexible system that can model different types of systems in networking, computer bases, and other applications. It uses mathematics to model dynamic systems and formal analysis of the behaviour of system models based on performance. The PN concept comprises four parts: place (showing the resource of the system), transaction (an event that happens to transfer data), token (number of resources, which is called marking in the network model) and arc (direction of the system), which connects the place and the transaction. Finally, a Platform Independent PN editor, which is Java based and is used to simulate the data flow model, is added to the modelled system. Figure 3.14 shows the data flow model and is explained in the following section.

As shown in Figure 3.14, the PN model include four areas: hospital, home, emergency and open areas. All submodels involve sending a request, receiving a request, firing, processing, and receiving a response. The initial marking (token) involves five places, each of which has

a token: DR (doctor), NUR (nurse), SEN (Body sensor), ENVS (environment sensor) and INS (insurance company). The model is initiated by the DR or NUR, who sends a request to monitor data. By firing transaction number 1, the token from DR and NUR is forwarded to CU4. After processing by CU4, transaction 18 fires to take the token from SEN4. After processing by the CU, the token is forwarded to the medical server by firing transactions 2 and 4. The environmental element is also forwarded to the medical server by firing transactions 3 and 4 to be recorded in the medical server. Finally, a new token (data) is forwarded to the CU by firing transaction 19. DR and NUR can check the data and, after updating the token response to SEN, can provide new services. The token from INS is forwarded to the medical server after firing transaction 4 to receive general information about the patient. After firing occurs in transaction 6, the request from NUR3 is forwarded to CU3 at home. NUR can apply new services, which can respond by firing transaction 21. CU3 and ENVS3 tokens are forwarded to the medical server after firing occurs in transactions 7, 8 and 12. The token is recorded in the medical server and responds to SEN3 at home by firing transactions 26 and 20. The existing token is updated after the token is received by CU3. Finally, a new token is transferred to SEN3 when transaction 21 is fired.

In the emergency area, initial marking (token) is involved in three places (DR2, NUR2 and SEN2), each of which has a token. Based on the assumptions of the data flow model in this research project, DR or NUR sends a request to CU2 by firing transaction 13 or 14. In this model, the token from SENS2 is forwarded to the CU by firing transaction 23. Based on the new token, NUR or DR publishes new services, which are received by SEN2 after firing transaction 23. The token is also forwarded from CU2 to be recorded and checked by another healthcare service provider in the hospital by firing transactions 10, 17 and 12. A new token from another external user can also apply to CU2 after transactions 16, 22 or 26 and 22 fire.

In the last model (open area), any healthcare service provider can send a request to CU1 by firing transactions 26 and 24 from the hospital or transactions 16 and 24 from external users. After processing by CU1, the token is forwarded to SEN1 by firing transaction 24. SEN1 sends a response to the healthcare service provider by firing transaction 15. New processing occurs when the token reaches the CU. Based on the new token in CU1, the physician will publish new services that apply to SEN 1.

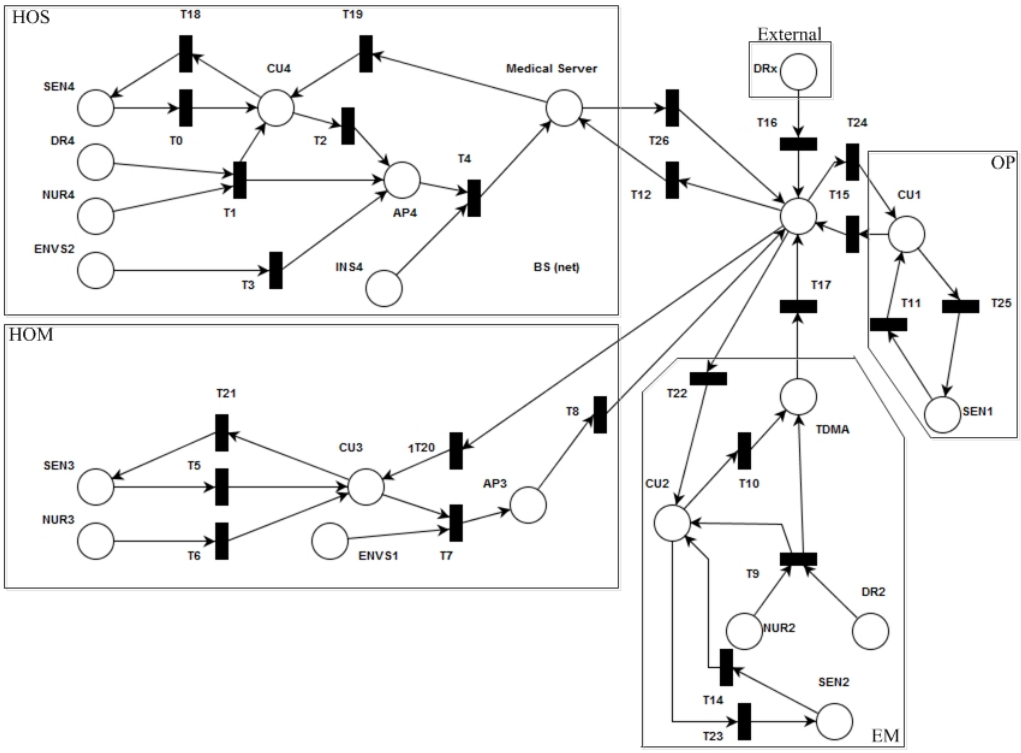

Figure 3.14: Data Flow Model Based on Hospital, Home, Emergency, and Open Area scenarios

The aim is to analyse and check the properties of the data flow model presented and to provide an accurate result in relation to boundedness, safety, deadlock, and liveness and the state space report generated investigated. Based on the proposed model, deadlock will happen when dead marking appears in the system model. Dead marking will also happen in the system model when a transaction cannot fire the transfer token into the next place. Strongly connected components (SCC) check the reachability of the model. Reachability in SCC means that a node must be connected to another node while receiving or sending tokens. SCC is also used to test and check an existing loop in the system model when marking firing by transactions. If the number of SCC nodes and number of arcs between nodes in the system model are similar, the transaction in the system model is without livelock. The full state report for this model showed 286 nodes and 741 arcs. The SCC-generated report had 286 nodes and 741 arcs. This demonstrates that the proposed model has no livelocks or loops. According to the definitions, the system model is reachable because the number of nodes and arcs in the SCC and full state space are similar. The time sequence in both reports is equal to zero (0) based on the system model. This causes the home marking to show none and means that marking can be

available in the next place after firing transaction. There were zero live transmission instances and dead transition instances and four dead markings, which means that these markings cannot bind the transfer to the next place. This is logical because, when the server sends a request to the client, the server goes into an idle state while waiting for the client's response to the new message. These reports and existing data show that all transactions of the proposed model are free of livelock, which means that the system model is safe (reachable) and bounded and has no deadlock.

- **Illustration of Existing Attack Models on the Developed Data Flow Model**

In this section, different types of attacks targeting network and application based data are identified and presented.

Attacks targeting communication network: In the healthcare domain, passive attacks can cause life-threatening invasion of privacy. With critical shared data and various medical devices that are wireless in nature, attacks such as traffic analysis and eavesdropping can easily happen in BANs. The attackers steal medical data by eavesdropping on wireless communications while critical data are transferred from patient to medical servers or vice versa. In this situation, the attacker is able to compromise the patient's privacy by executing a crypt-analytical attack on the eavesdropped data.

There are various forms of active attack in the healthcare domain. Because of the wireless nature of the communication, a BAN is susceptible to classical attacks such as message modification, replay of recorded messages, man-in-the-middle and masquerade. As described in the literature, the attacker could attempt to compromise the sensor nodes held by the patient. A captured node in a BAN system can be manipulated to apply modifications and intercept attacks. Because sensitive and critical health data are stored and shared over the networks, it is possible for a number of eavesdropping attacks to happen at the same time and location, which is termed a collusion attack [Ahmad et al., 2015, Zhang et al., 2014a].

Attacks targeting the data and applications: An external user such as a physician needs to access medical resources to obtain medical information. This demand could open BAN communication to internet attacks. In such a case, an adversary would be able to send a query through the same ID and message authentication code address to compromise the CU. According to the initial authorisation between the sensor and CU, an adversary could access

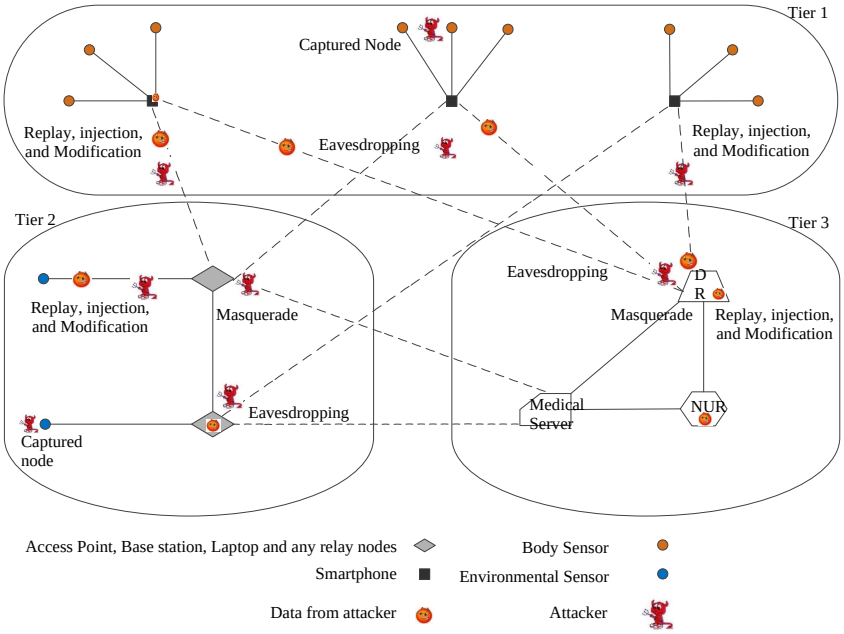

Figure 3.15: Attack scenario based on proposed model

the medical data in the CU. The CU could forward a query to the medical server or physician requesting further services, which could endanger the whole network. It is necessary to apply access control over users based on the variety of roles, policies and access levels to prevent or limit this type of attack and unauthorised access.

Multiple physicians in the same or different locations present a diversity of roles and policies in the proposed model. An adversary may be able to attack devices that are held by a physician (e.g., a smartphone). These devices are in communication with other base stations to monitor medical data in real time as required. As a result, an adversary could endanger critical data recorded in the different medical databases. An adversary might also access all the medical data in any location via the doctor's device because the doctor has full permission to access the medical resources. It is important to maintain control over who has been granted access to write and read the shared data in networks. Authentication and secrecy attacks enable the execution of attacks such as impersonation, which may compromise the patient's privacy. Authentication and secrecy attacks cause threats such as location and activity tracking, which can be a disaster for information shared in networks. By sending extra redundant packets, the simplest type of denial of service attack attempts to use up the resources available to the node under attack.

An attack at the beginning of the sensor deployment in a BAN network is an important issue that has not been addressed in past studies. An adversary could attack patients at the beginning of a network and might obtain critical security parameters such as shared keys. Finally, the attacker might access recorded medical data, which could threaten a patient's health or life. Such attacks might deplete the battery in a sensor which is not suitable for BAN. Several types of malware, such as Cajino and Vdloader, are available on new smart devices such as Android smartphones and can transfer data to the internet using different mechanisms such as 4G. These types of malware may be able to open a back door or install applications in attempts to change access levels of different users, steal confidential information or compromise devices, which may lead to life-threatening situations [Al Ameen et al., 2012].

3.3 Summary

A data flow model was developed based on four general healthcare scenarios. First, the assumptions of the model (responsibilities, roles, policies, topology, etc.) were introduced and used to show who, how and from where medical data can be accessed. Based on the assumptions and extensive literature (communication, topology, technology, etc.), a data flow model was developed and the accuracy of each model was investigated in a UML sequence diagram. PN software language was used to analyse the behaviour of the proposed model. The use of the UML sequence diagram and PNs, which enable formal analysis by creating a graphical shape, helped in the critical review of the design and during modelling and testing. Finally, attack models based on the data flow models and BAN architecture were identified.

The scenarios from factual life and indoor and outdoor healthcare models showed that these environments are very complex and the data flow models are to be designed specifically for each use, especially to support the diverse parties involved. Based on these scenarios and the data flow model developed for indoor and outdoor healthcare, all domains require different authorities to manage different parties in their location. Thus, different authorities must interact with each other in a medical BAN architecture. This research project has proposed different ways to populate sensor networks to support indoor and outdoor healthcare environments based on the network architecture. Communication in indoor and outdoor environments based on different authorities raises serious privacy concerns for BANs.

This chapter has presented a deep conceptual data flow scheme to describe the different parties and environments, and how the data are input and transmitted to other places as part of the output. This chapter has described the arrangement of different tasks and duties, their limitations and the effects of these limitations on data transmission using formal language (PNs). The PN results showed the relationships between different parties and environments, and showed that the model worked well. This formal modelling can be used to understand data flow when dealing with a variety of access requests such as from doctors and nurses. In this case, the authenticity of data flow based can be identified for the defined scenario. This formal model will help verify the correctness, availability and integrity of the model developed. The results confirmed that the described properties were acceptable and that all transactions in the model activated and terminated acceptably.

The model developed in this research study presents for the first time a unique model to support monitoring by any users based on individuals and groups of people in indoor and outdoor environments. The critical vulnerabilities identified in the model comprise important factors that can influence the usability and acceptability of BAN-related products in the health domain. It is an independent model that can be used to generate secret keys to secure communication and to provide appropriate access control mechanisms based on users duties. The next chapter begins with a simple example of the relationships between users based on the data flow model developed. The chapter then introduces an access policy model to provide an appropriate policy for users. The model is acceptable for users, regardless of location and wherever they move between locations as a function of their duties.

Chapter 4

Access Control Policy Model

4.1 Overview

In the data flow model developed in this research study, healthcare systems include different stakeholders such as patients, doctors, nurses and insurance companies. As explained in Chapter 3, stakeholders in the healthcare model have different relationships with each other. The general overview of sharing health data and the relationships between stakeholders in the data flow model developed in this study are depicted in Figure 4.1.

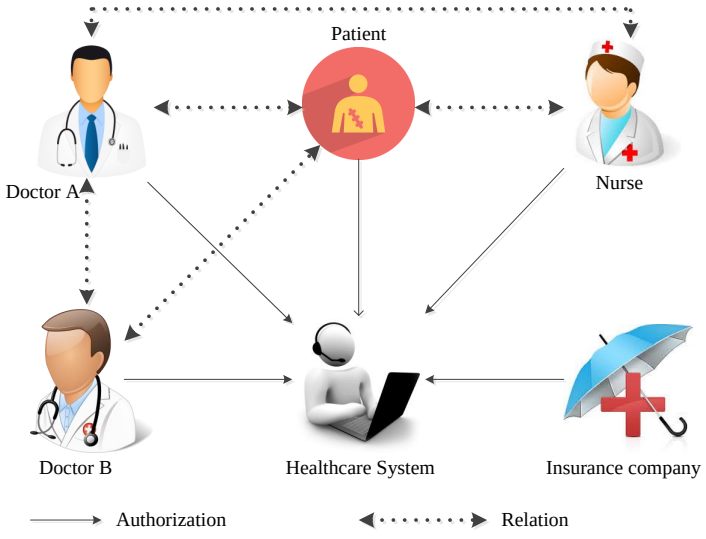

Figure 4.1: Sharing data and the relation of stakeholders

As seen in Figure 4.1, doctors A and B and doctor A and the nurse cooperate closely with each other to share information and to monitor the patient. Doctors A and B, and the nurse, patient, and insurance company have access to the healthcare system with different levels of authorization and permission. Different level of access and permission are assigned to stakeholders according to their roles, responsibilities, location and duties. For example, the patient can see his/her profile and update general information. The insurance company can access general data. To ensure high-quality access to sensitive data recorded in the healthcare system, an access control model based on the role-based access control (RBAC) model is needed. As defined by the RBAC, the roles and permission are given to different entities in the model presented, which helps us to provide an appropriate policy model to achieve to the objectives of this study.

According to data flow model developed in this study, the stakeholders share data and access sensitive data from different environments such as the home, hospital or emergency vehicle. Models reported in the literature include the modified RBAC [Zhang et al., 2002], context-aware access control (CAAC1) [Garcia-Morchon and Wehrle, 2010a] and criticality aware access control (CAAC2) [Gupta et al., 2006, Venkatasubramanian et al., 2014]. A few models apply only the role in their access control policy models (RBAC), whereas others restrict the role and permission tasks according to their context (CAAC 1 and 2). The existing role-based access control models are based on a static constrained RBAC model, which is unacceptable in emergency and open area environments because the healthcare service provider needs to access medical data at any time and location according to their roles, responsibilities and context. Health professionals need to have new authority to access sensitive data, which is called delegation. Some models, such as CAAC 2, are applicable for use in emergency situations. In these models, the value of the data collected are compared with the policies defined by the administrator. These models do not consider the usability of CAAC 1 in emergency situations. Both the context model and RBAC model were integrated into the model developed as part of this research. This provides a suitable access control policy model based on the stakeholders roles, responsibilities and context.

The necessary security requirements identified in the model developed in this research are as follows.

A- Each domain, such as a hospital, home or emergency vehicle, must establish their security

requirements and policy.

B- Each professional staff member must have the ability to define the policy for new files in critical situations.

C- Patients must have control of their medical data and be able to grant new access to healthcare service providers.

D- The handling of policies and access control should be easy for patients and medical administrators.

E- Different levels of security policy and access must be defined for users according to their location and responsibilities.

4.2 Overview of the Access Control Policy Model

According to the data flow model developed and presented as a general model (Fig 1), the patient data are shared between different healthcare environments, and healthcare service providers must be able to access the data. The administrative authority must predefine the policy and grant access permission to users in order for them to access the system at any place and time. The policy and permission should be adaptable according to the healthcare environment, which should help improve the responses in both normal and emergency situations. Access to patient medical data is ensured if and only if the user's permission satisfies all of the policies.

To provide suitable access control model to represent a patient's situation, the model investigated different security levels based on stakeholders situation. The critical situation is important because the patient's life may be in danger, and the security level is high. To prevent threats to the patient, the professional staff are assigned directly in the health device or system without delay so that they can monitor the health data in real time in place. After the health issue addressed with the particular healthcare service provider, critical level of access shift to serious level of access. At this level, the healthcare service provider can access the medical server and monitor the recorded data to check the patient's condition frequently. The staff can access data from other locations and departments to ensure the patient's safety. This allows the stakeholders to change the serious mode to critical or normal based on the recorded data. A serious level of access shift to normal or critical level of access based on the new report. In the normal mode,

the professional staff members can access some data if authorized. According to the scenarios presented, when dealing with a critical or serious condition, some professionals may need to access health data for which they might not be authorized.

In addition, practical permission must be assigned to professional staff member attributes to prevent information leaking while still providing full access to health data at all levels of access described above. For example, a surgery department may have many staff members working at same time. It is important to provide appropriate access at the right time for all staff members to prevent any conflicts and information leaking in the system. To do this, it is better for the administrator to grant access to physicians to collect and analyse the medical data. This can be followed by development of a profile with different access levels created for each healthcare service provider to then monitor the data. In this model, granting access only to those staff members with a particular profile will help to optimise treatment and prevent information leaking.

There must also be a high level of control monitoring of professional staff members that can control their permission but allow them to access the medical data readily from different places both day and night. To do this, the requested access should be examined to find similarities and differences between the right authorizations to access a particular resource and the main profile fixed for each patient. Access to medical data is given to specific staff members if and only if the permission in both the patient profile and professional staff is equal. This will reduce the risk of inappropriate access to medical information in healthcare environments.

This section discusses the basic RBAC concept and how it can be used to determine access policy, role, and users responsibilities in the data flow model developed (Fig 4.2) [Shin et al., 2015], [Sandhu et al., 2000], [Zhang et al., 2003] used and modified.

RBAC relation flow diagram includes, roles, users, permission, and contexts, in which the users are assigned a role, which is called user assignment. Each role is connected to a permission, which is called permission assignment. The relationship between roles in the RBAC system is called role hierarchy (RH). Figure 4.3 shows a sample RH. In this example, doctors (DRs) 1 and 2 inherited their role from the healthcare service provider. DR1 has responsibilities at hospitals (HOS) 1 and 2, which includes departments (DPs) 1, 2, 3 and 4. DR1 from HOS1 has access to patient (P) 1 (relationships in both DP1 and DP 2). DR1 has also access to P2 in HOS2 (relationships in both DP3 and DP4). The scenarios for DR2 are similar to those of DR1

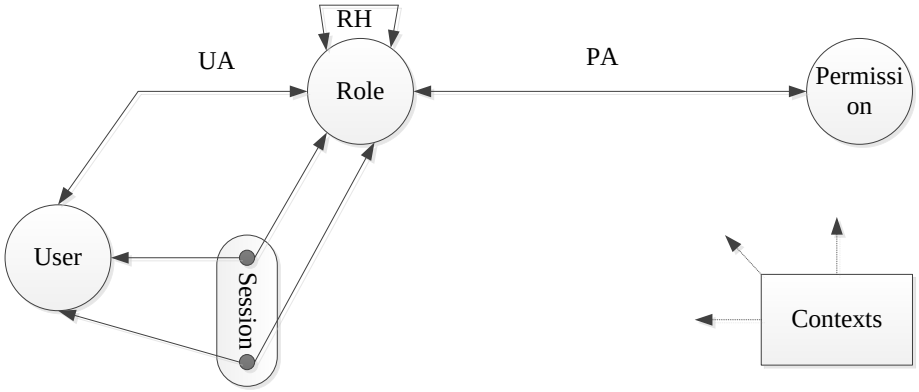

Figure 4.2: RBAC relation flow
Sandhu et al. [2000], Zhang et al. [2003], Shin et al. [2015]

by different situation as depicted in Figure 4.3.

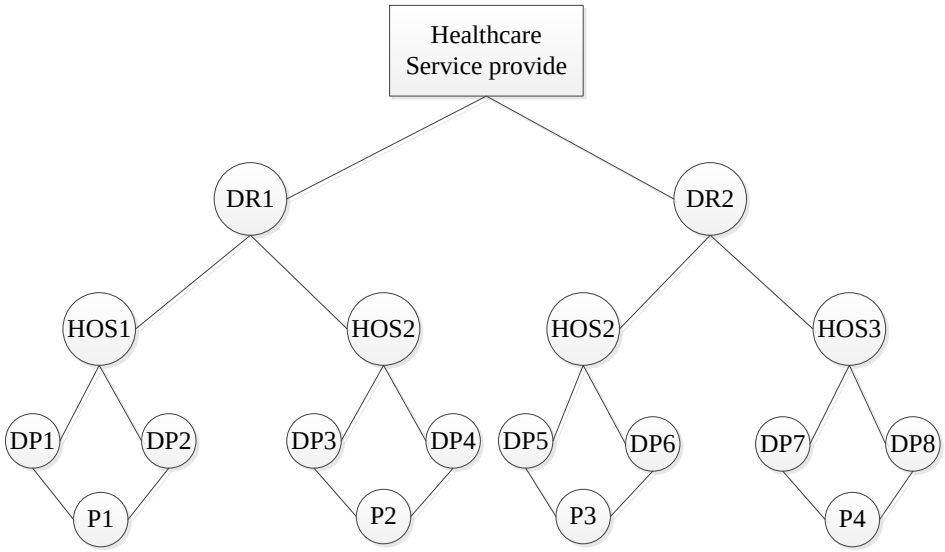

Figure 4.3: Framework for RBAC based on developed data flow model

To provide a suitable access control policy model based on the data flow model developed, a proposed framework was created by modifying the concept of RBAC [Shin et al., 2015], Sandhu et al. [2000], Zhang et al. [2003], as shown in Figure 4.4. In this framework, additional data such as contexts, environments (e.g., home and hospital), situation (emergency or normal),

subjects (patients) and objects (healthcare service providers) were needed. The access profile needed to record all related data about the objects and subjects, which helped the permission system realize the object and subject requirements. Finally, the permission file was divided into two parts based on low and high relationships between the requested data from objects or subjects and the availability of data in the permission file. If the relationship with the received data differs from the recorded data in the permission file, the request is rejected. Otherwise, the requested data is used to estimate the correlation. If the result is high, the permission is refused with conditions. In this case, the system checks the information from the permission file and accesses the profile to finalize the access. If the result is low, access is granted to the subject or object. The relationships between the user, session and roles described above are depicted in Figure 4.4. Thus, the concept of presented framework used to provide appropriate access control model regard to developed data flow models in this study. This will help provide a basic access control policy model.

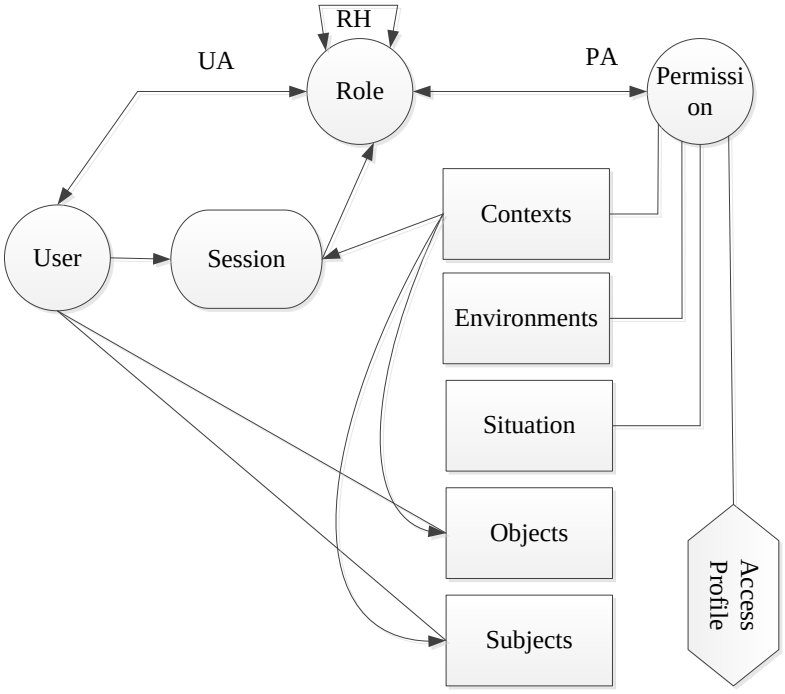

Figure 4.4: RBAC framework based on data flow model

According to data flow model and framework presented (Fig 4.4), official permission is an important issue for the subject and object. The first issue is that healthcare service providers and

patients may not be in same location and will therefore have different security requirements for their domains. For example, a doctor from one hospital needs to access to patient A's medical data, but patient A is at the university hospital. When different healthcare domains and environments are involved and have different requirements, different controls must be set according to their domains. Each domain must have specific security requirements because the attributes may be specific to each domain. Therefore, some security issues must be marked with an address to provide efficient control for both subjects and objects in healthcare domains. Firstly, healthcare service providers need to have a high level of control. Secondly, user attributes must be protected. Thirdly, the privacy of the new service requester must be protected from the domain manager. This means that it is not necessary for the domain authority to access the third party service requester. To prevent users without authorization gaining access and recording data in the access profile, the new third party requester, as a subject or object, must obtain permission from the system.

Finally, to illustrate the relationships between different parties in terms of their requests and responses in the presented data flow model and framework, the models extends according to the part of appropriate mechanism, which is called eXtensible Access Control Markup Language (XACML). XACML is a standard access control policy language [Parducci, 2005]. The policies in XACML were implemented in Extensible Markup Language, which converts a message with a set of roles into a code with a specific structure and format. This standard was made by The Organization for the Advancement of Structured Information Standards in 2005 [Parducci, 2005]. XACML is a promising mechanism for evaluating and testing a variety of access control to resource in the healthcare area based on the roles and responsibilities, which are determined based on defined policies. This project investigated XACML as a general propose to fit the standard based on the framework and data flow models presented. In general, this standard comprises a query and response structure, ruling system, functions, and database. The XACML access control framework used in the data flow and access control policy models is depicted in Figure 4.5.

As shown in the framework depicted in Figure 4.5[1], the proposed framework includes components such as the policy retrieval point (PRP), policy administration point (PAP), policy decision point (PDP), policy enforcement point (PEP), policy information point (PIP) and context handler (CH). The PIP is one of the forceful modules in the XACML framework that

[1]S: Step

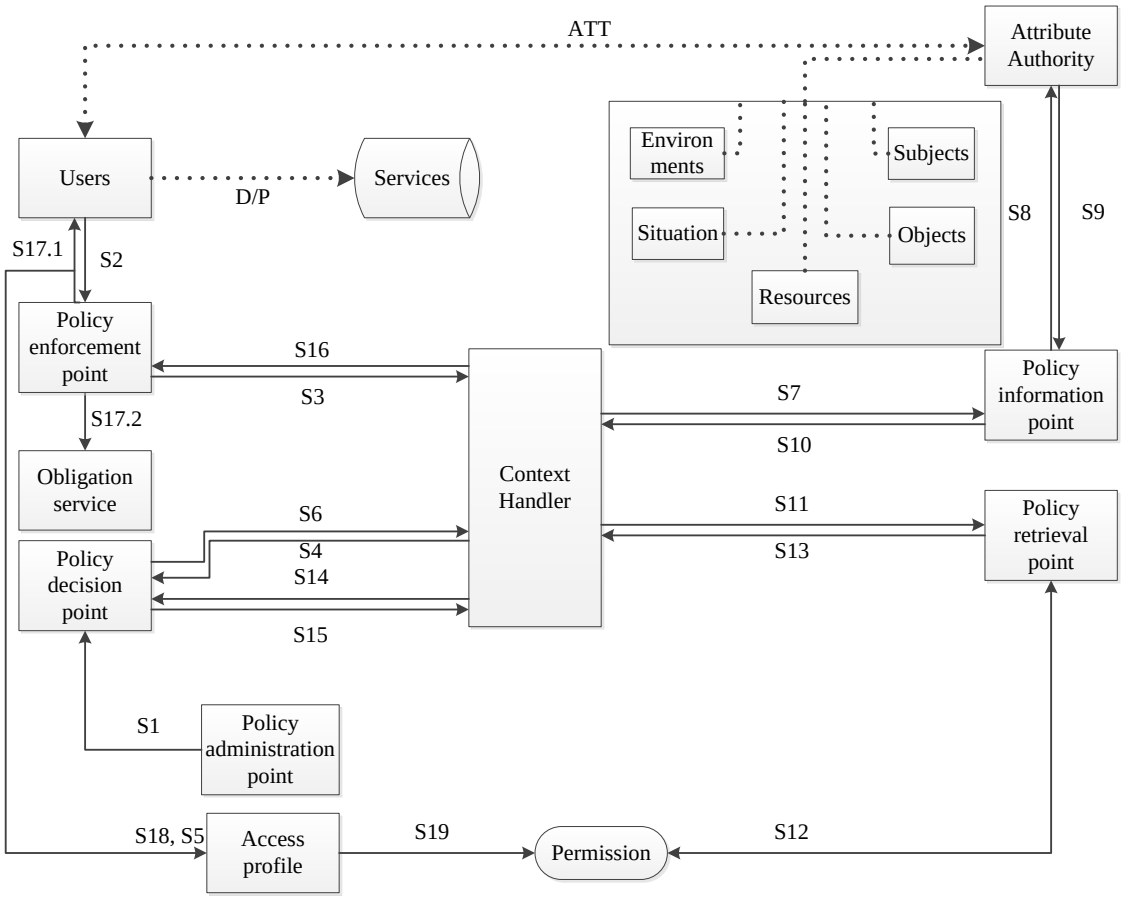

Figure 4.5: XACML Access Control Framework Based on Data Flow Model

encapsulate and collect all attribute values from environments, situations, subjects, objects and resources. In this framework, the PIP obtains all necessary information and forwards it to the CH. The information such as attributes is gathered from the subcomponent by the attribute authority (AA) and then the collected information is sent to the PIP based on new requests.

The PRP is a database that records and stores all access policies and is considered as a module for conclusive different level of permission. When conclusive the different level of permission, the PRP obtains the demanded data (e.g., the information about different level of grant to resource). In the model developed here, the PRP collects the information from the PIP and decides new access permission by using data from the permission database and then forwarding the new information to the PDP. The PDP is an important component in the access control policy model that, before granting access to users, evaluates and makes a firm decision about the requested access according to the policies using valid data such as attributes and the

security levels.

The PAP is a step in the administration of all policies with regard to authorization of users access to critical information. This step must be able to manage the PDP with separate policies and possibly with multiple PDPs. The PAP must be able to use different policies and store data at the same time that the user requests service. First and final step in the model is the PEP. After the request to evaluate and grant permission based on a set of policies and roles, the PEP delivers the response to the users, permits or denies access to new information and forwards the access profile and permission to further services. The following subsection discusses the request and response flow, which expanded this standard by using the RBAC and data flow models presented.

4.3 Analysis of XACML Model

In the first step, the initial roles and policy sets are stored in the PAP, which allows the administration to control and administer all access. In the next step, the user sends a query to obtain permission to read health data or to access some medical resources as required. This query is received by the PEP and then forwarded to the CH. To evaluate the query according to the existing policies in health system, The CH transforms the query into XACML and forwards it to the PDP for a new decision. After the query is analysed, the PDP forwards the response to the PEP if and only if the requested data already exist in the database. If not, the PDP sends a query to the CH to obtain the new attributes and information. The CH forwards the new query from the PDP to PIP. The PIP processes the request and forwards the new query to the AA to collect the new information from subcomponents in AA domain. The collected data are then delivered to the CH. To set and verify the permission, the CH sends a request to the PRP. The PRP examines the new collated data obtained from the AA and then sets the new permission. In step 14, the CH forwards the new version of the data with new permission to the PDP for a final decision. In this step, the new information is evaluated and the access request is checked against the existing policies before final access is granted to the user. After the PDP decides on a new applicable policy, the new decision is submitted to the PEP. The PEP is the final step in making the final decision about whether a user is permitted or denied authorization.

4.4 Policy Model

A set of policies based on XACML policy was used to supply a suitable access control model based on the data flow model developed. The structure of the policy model is considered as a tree. The policy model for XACML is depicted in Figure 4.6. As shown in Figure 4.6, the policy structure includes PolicySet, Policy and Rule, each of which includes different components and subcomponents. As shown in Figure 4.6, XACML has a number of components and subcomponents in a hierarchical relationship. Based on the main idea of XACML, the PolicySet was used in the model presented used to cover all existing policies and other policy sets.

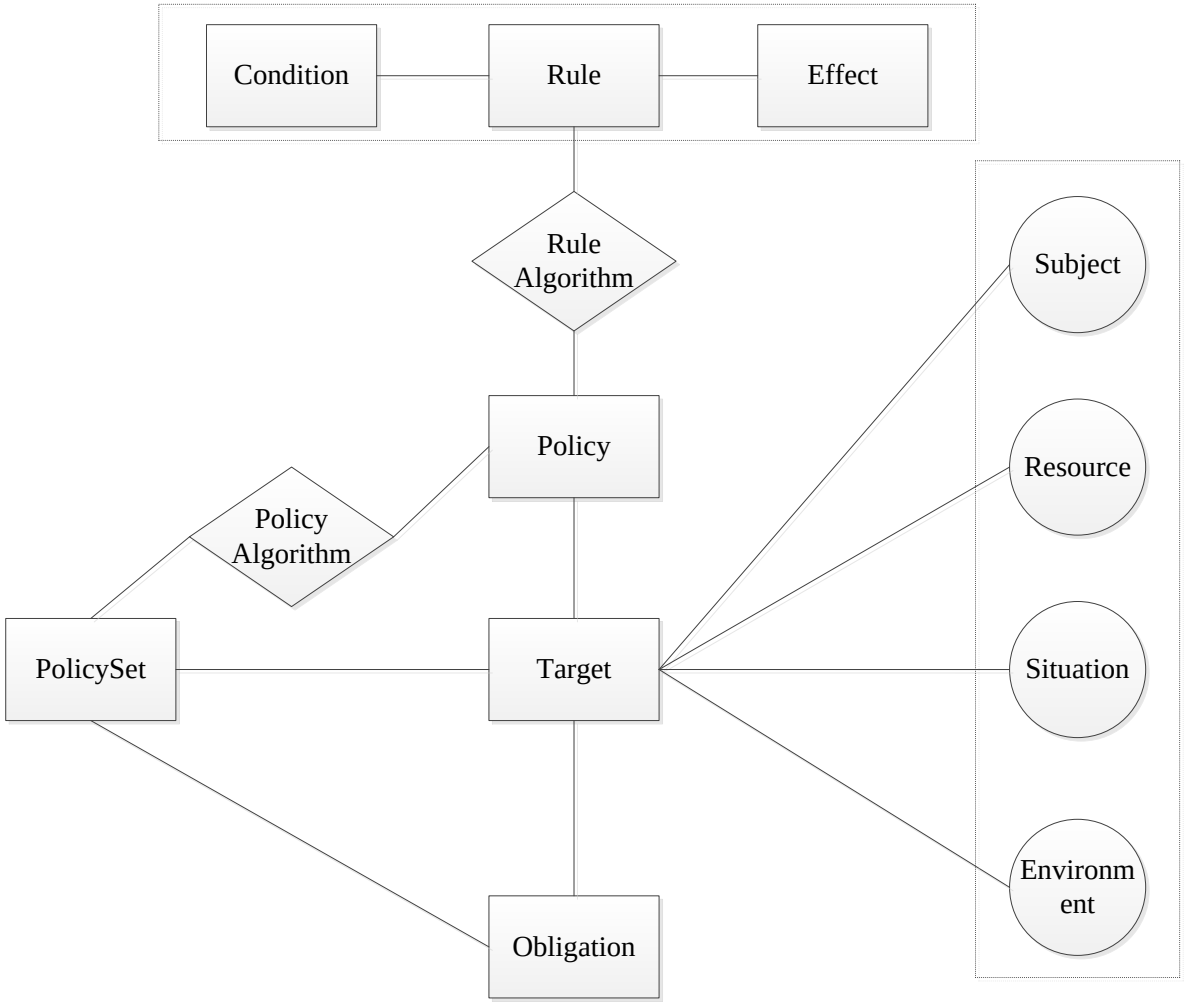

Figure 4.6: Policy Model based on XACML

Rule is the deepest component of this policy model. As shown in Figure 4.6, a number

of rules can be involved in a policy as components and subcomponents. The rule component comprises condition, target, and effect subcomponents. The subcondition component provides some restrictions on the XACML model to filter the outcome of access control. The result of condition is T (True) or F (False). The result of condition with the target component helps to supply an appropriate response for a subject based on the policies and their relationships. The effect component includes two characteristics such as permit services and deny services.

Another component of the policy model is target. This element is used to set boundaries such as the environment, situation, resource and subject. The relationship between different components in target is hierarchical, as is the relationship between target and its parent. The definition of target provide suitable rules based on existing elements. The subject subcomponent includes all characteristics of the subject that can be used by the CH for granting permission to the requester. The resource subcomponent includes a value of resource that gives an account of the value of the resource. This value is compared with the values for the subject in the CH to control the subject's access. Another subcomponent is situation, which includes values about the subject that are executed in relation to the resource. The final subcomponent of target is the environment, which includes all values for the environment.

The last section of this model is policy component. This section includes several rules and the target section, in which the target is used to filter the existing rules based on the subcomponents of target. As depicted in Figure 4.7, this component includes target, obligation and the algorithm that combines the existing rules. The rule algorithm is used to prevent any conflicts in terms of different rules. PolicySet is the root of policy model with PolicySet and policy subcomponents. The main function of this component is the organisation of different policies based on their subcomponents. These policies might be provided with different domains, but the outcome is a unique policy. A diagram of PolicySet is depicted in Figure 4.8.

According to policy model presented, the target component is evaluated and used at each step in the process of granting access in the access policy model. As a result, if and only if the PolicySet based on the target component is F, then the rest of the components and subcomponents would be F and deny would be returned to the CH. In addition, if and only if the subcomponents at the target match the existing attributes in the permission system and requester, the new policy sends to the deepest child.

Finally, the access permission is granted based on these attributes. The subjects must satisfy

the policy according to the attributes to access sensitive data.

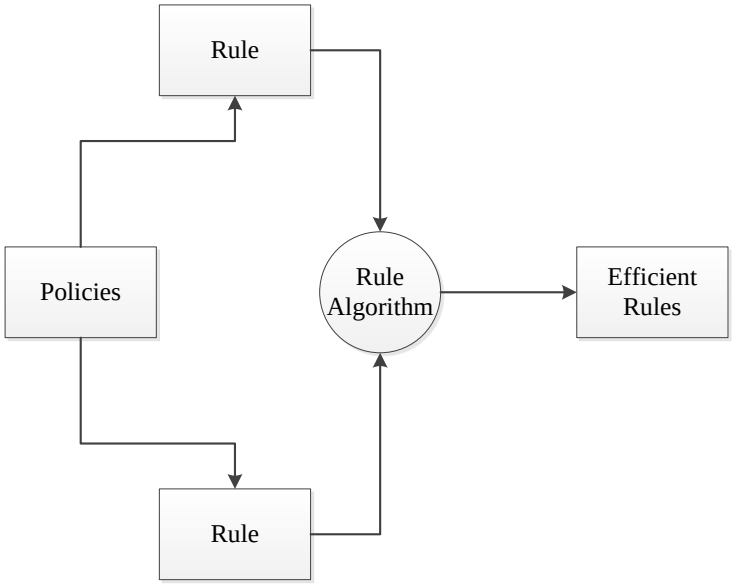

Figure 4.7: PolicySet framework for combining rule

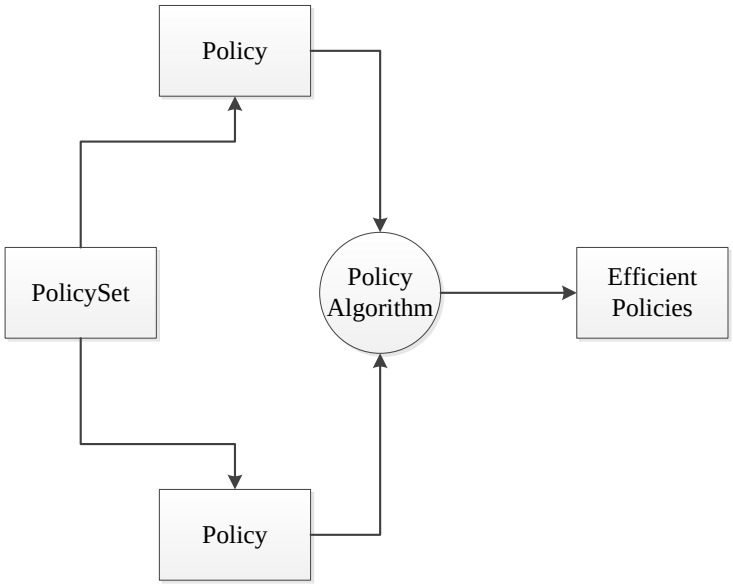

Figure 4.8: PolicySet Framework for Combining Policies

4.5 Analysis of Policy Model

The policy model designed and presented was based on the data flow model and access control policy framework developed in this research project. The policy model appears to have a strong ability to match the different attributes. The model designed provides an access policy for different subjects based on their attributes in terms of their responsibilities and duties, and the rules; the responsibilities and duties can change according to the location and user's requirements. Figure 4.9 illustrates how the check-and-verify policy model was based on concept of XACML. As mentioned earlier and shown in Figure 4.9, the policy model included policies, for which PolicySet is the top level and the relationships are depicted as a tree structure. Each PolicySet can comprise different trees and subtrees, as depicted in Figures 4.6, 4.7 and 4.8.

According to Figures 4.6, 4.7, 4.8 and 4.9, each PolicySet as a main root includes policies and targets, and the policy component has many leaves such as rules and targets. Finally, each rule includes a number of subcomponents such as target and condition. It is vital that these subcomponents are filtered and evaluated using existing and new policies based on any attributes. As depicted in Figure 4.9 and as described earlier, the target included four subcomponents. The main idea is that the attributes from requester (<XACML-CH: Requst>) must match and satisfy at least one of the defined policies in target components (<Target>). The target would check for similarity with the matched attributes and publish F if and only if none of the attributes match the existing policies. The subject components comprise (<SubjectMatch>) subcomponent, which is evaluated against the existing attributes in the CH. The resource, situation and environment comprise in sequence (<ResourceMatch>), (<SituationMatch>) and (<EnvironmentMatch>) subcomponent. Each (<SubjectMatch>), (<ResourceMatch>), (<SituationMatch>) and (<EnvironmentMatch>) comprise: firstly, the attribute label related to each subcomponent is called (<XACML:AttributeValue>). Secondly, each component of the target includes several attributes. To separate and isolate each attribute, a new tag called (<AttributeDesignatorT>) is used to keep different elements with different values. To match all values based on different subcomponents, (<AttributeSelectorT>) is used. Finally, the condition component is used to evaluate the outcome of each target for each requester. The main target of condition is to filter one more time the attached attributes from requester and target before sending to the CH for a final decision.

According to the access control policy framework presented, the PDP checks and investigates the different requests based on the incoming request from the subject and then evaluates the elements whose characteristics differ from the policies defined in the system (target, effect and condition). In this step, the target at different levels is processed to filter the results. Each target woks as a condition and precondition for any subtarget. This means that the result of the deeper target is evaluated according to the upper target or precondition in relation to the requester's attributes. To give an example of how the policy model works, a sample is described in the following of paragraph.

Dr Reza needs to access to the profile of Mr Ali, who is ill. The administrator defines Policy 2 for access to sensitive data about Mr Ali. According to this policy, the subject must be a doctor employed in the surgery department of Beheshti Hospital. Because the privacy of recorded data is important, the administrator defines Policy 2 under Policy 1, which makes Policy 2 a subpolicy of Policy 1. The subject must be registered in Medical 1 from Brisbane, Australia. According to the policy model presented, information at the level of the subject is executed in PolicySet Target, and the information for Policy 2 is executed in PolicySet rule. Thus, the subject (Dr Reza) can access sensitive information if and only if the attributes satisfy Policy 1 or Policy 2 is accessible if and only if the result of Policy 1 is T.

4.6 Summary

This chapter introduced an access policy model that was developed, based on the characteristics presented and identied in Chapter 3, to create a data ow model for WBAN in the healthcare environment. In addition to supporting the model characteristics, such as role, session and permission, the RBAC model was used to check the old permission and user activity before creating a new permission. In addition, the concept of XACML was used to propose an access control framework that could t the data ow and also the RBAC model developed. Some factors such as rules, targets and policies were identied, and these helped to lter the access based on user attributes and other components such as the environment, resources, and satiation. The extended language also supports the representation of tasks and task instances. It proposes new a policy set, called PolicySet, to prevent conict with the nal decision regarding multiple roles and responsibility, which can be assigned to the same user. The XACML model also supports separation of duties and binding of duty constraints at the level of process instances.

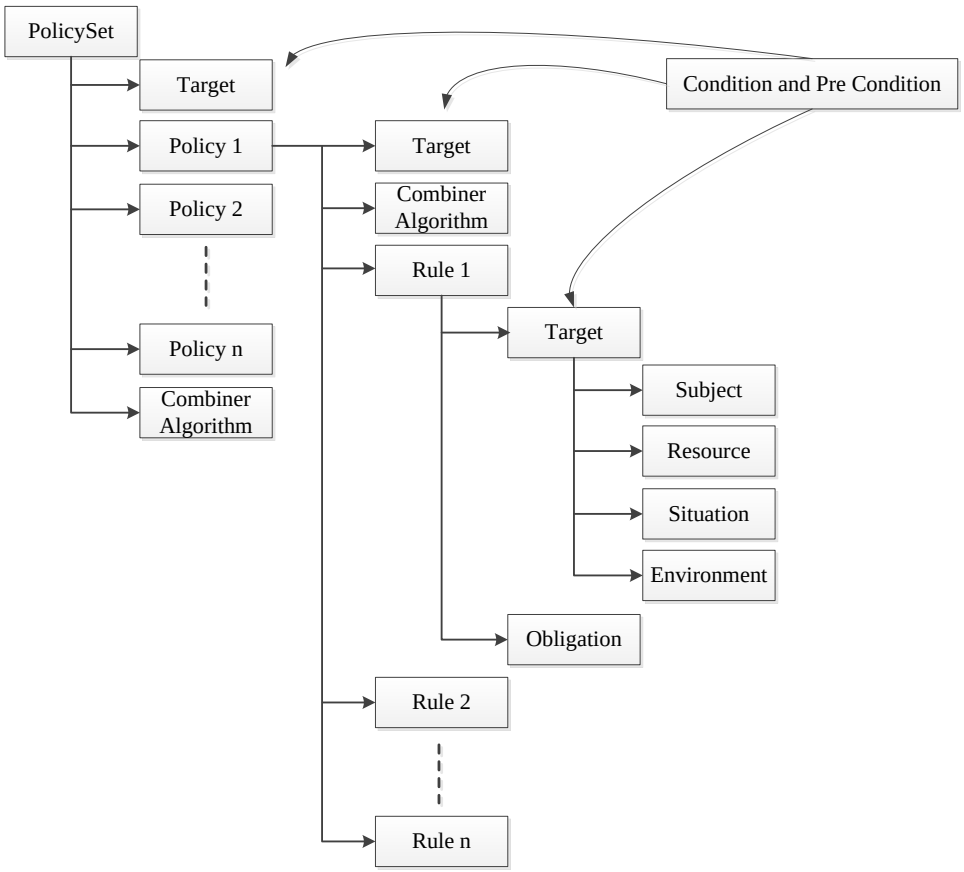

Figure 4.9: Policy Workflow Framework

The new PolicySet supports the representation of instance-level restrictions in a way that can be linked to the related tasks, and can be evaluated. This model can protect sensitive data against unauthorized users by using the different policies as presented. Using the concepts of XACML and RBAC, this project has designed a framework for healthcare systems, using the characteristics from Chapter 3 and 4, to be able to support authorisation policies for any workow authorisation model.

In the next chapter, this thesis will present the conclusion and future work. The conclusion will elaborate on the contributions of this thesis by outlining them explicitly. The future work will consist of possible research problems to investigate arising from the outcome of this research.

Chapter 5

Conclusions and Recommendations

5.1 Overview

This chapter reviews the purpose and objectives of the project in the order presented in earlier chapters and proposes mechanisms for the application of the models developed in this research study.

5.2 Summary of the Research

Many researchers throughout the world have established different electronic healthcare services to provide a suitable platform for sharing critical information about patients through open networks. These platforms should help various user groups from diverse backgrounds, such as physicians, staff members and other healthcare services providers, to access medical information in real-time. Recent developments in different technologies such as mobile computing and communication allow users to move freely. Existing technologies help improve the quality of healthcare services and quality of life. However, transmitting and accessing health information using various environments and technologies present important challenges. To address these challenges, studies of data flow communications models have focused on individual patient monitoring in indoor environments. However, healthcare and remote healthcare monitoring of small and large groups in indoor and outdoor environments have not been addressed.

5.2.1 Summary of Outcomes and Objectives

This section discusses the outcomes of this thesis, as presented in detail in each chapter, and maps them to the specific research objectives as presented in Chapter 1.

Objective 1: To investigate and analyse wireless body area networks (BANs) in healthcare domains. A comprehensive literature review was undertaken to establish the background for the research problem, to identify gaps in knowledge and scope, and to validate the research methodology. As mentioned in the research plan and approach, many articles and survey papers from journals, conferences, books and technical reports were reviewed to prepare a research proposal and extensive literature review for this research project. Based on the initial research proposal, an extensive literature review was included in Chapter 2; this included background information about BANs in the healthcare setting; the types of applications in medical, military and entertainment settings; characteristics of BANs; types of communication and existing technology used in BANs; existing BAN architecture used in healthcare; existing problems in BAN applications; understanding the relationships between BANs in the same and different locations; and existing policy models related to healthcare.

Objective 2: To develop and verify data ow models for BAN applications in healthcare domains, different BAN application domains and scenarios for each medical domain were identified. In the context of the different domains and applications, a variety of stakeholders, such as patients, doctors, nurses, family members, and insurance companies were identified for each model. Different rules and responsibilities for each stakeholder were introduced based on each domain. The BAN architecture and security model were introduced and modelled for this research project. As a result, a data flow model for BAN communication under four healthcare environments (hospital, home, emergency, and open areas) was created. Unified Modelling Language was used to examine the model developed based on the different parameters discussed in Chapter 4. Petri Nets software was also used to model the data flow . Types of indoor and outdoor attack scenarios on data flow were identified and discussed. The attacks identified were classified as active and passive attacks from malicious insiders and outsiders, and these were modelled according to the model developed. The outcomes of objectives 1 and 2 were presented as a conference paper that was published in 17 IEEE HealthCom'15.

Objective 3: To develop an access policy model for BAN data flow models. In the data flow model developed for indoor and outdoor areas, the patient-related data is shared between different healthcare environments and healthcare service providers and must be accessed by users. In our policy model, the authority of domains predefine some policy and grant permission to users to access the system from any place and at any time. A policy model and framework with respect to different attributes of the subject, object, environment, situation and their recourse are recommended using the concept of eXtensible Access Control Markup Language. The policy model developed in this research allows a quick response to any healthcare service provider. An access profile was designed to control the users through a predefined policy controlled by the administrator of a healthcare system. The entire history of actions, including access, types of permission and locations of requesters are recorded, and this history can help the administrator improve the policy. The concept of role-based access control can be used to provide the access profile and permission to filter the new policy.

5.3 Future work and Recommendations

This section suggests possible opportunities based on the outcomes of this thesis that may be considered for future work.

1) Develop key management models for BANs related to the data flow models developed. According to the data flow model developed in this study, each environment includes a controller that can manage people in their areas. Therefore, there are different ways to generate secret keys based on a variety of domains and administrators. To secure communication and data collection between various entities in and around BANs, suitable technology must be developed to maintain a high level of security and practicality as a foundation for healthcare monitoring. Key management techniques need to be developed for managing and distributing keys to stakeholders and open networks.

2) Develop access control models for BAN data flow and key management models. Our model included different environments with different controllers to manage the uses. To monitor patients in real time, users must access medical resources in different domains. Efficient access control models are needed to grant permission for accessing a patient's

profile and to provide privileges for a particular set of users at different times and locations.

Literature Cited

Acampora, G., Cook, D. J., Rashidi, P., and Vasilakos, A. V. (2013). A survey on ambient intelligence in healthcare. *Proceedings of the IEEE*, 101(12):2470–2494.

Ahmad, S. S., Camtepe, S., and Jayalath, D. (2015). Understanding data flow and security requirements in wireless body area networks for healthcare. In *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, pages 621–626. IEEE.

Akyildiz, I. F. and Vuran, M. C. (2010). *Wireless sensor networks*, volume 4. John Wiley & Sons.

Al Ameen, M., Liu, J., and Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, 36(1):93–101.

Aminian, M. and Naji, H. (2013). A hospital healthcare monitoring system using wireless sensor networks. *J. Health Med. Inform*, 121.

Ardagna, C. A., di Vimercati, S. D. C., Grandison, T., Jajodia, S., and Samarati, P. (2008). Regulating exceptions in healthcare using policy spaces. In *Data and Applications Security XXII*, pages 254–267. Springer.

Asada, G., Dong, M., Lin, T., Newberg, F., Pottie, G., Kaiser, W., and Marcy, H. (1998). Wireless integrated network sensors: Low power systems on a chip. In *Solid-State Circuits Conference, 1998. ESSCIRC'98. Proceedings of the 24th European*, pages 9–16. IEEE.

Bettini, C. (2002). Obligation monitoring in policy management. In *Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on*, pages 2–12. IEEE.

Brown, J, E. (2012). Medical body area networks @ONLINE.

Cavallari, R., Martelli, F., Rosini, R., Buratti, C., and Verdone, R. (2014). A survey on wireless body area networks: technologies and design challenges.

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., and Leung, V. C. (2011). Body area networks: A survey. *Mobile networks and applications*, 16(2):171–193.

Custodio, V., Herrera, F. J., López, G., and Moreno, J. I. (2012). A review on architectures and communications technologies for wearable health-monitoring systems. *Sensors*, 12(10):13907–13946.

Darwish, A. and Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, 11(6):5561–5595.

Drude, S. (2007). Requirements and application scenarios for body area networks. In *Mobile and Wireless Communications Summit, 2007. 16th IST*, pages 1–5. IEEE.

Felisberto, F., Costa, N., Fdez-Riverola, F., and Pereira, A. (2012). Unobstructive body area networks (ban) for efficient movement monitoring. *Sensors*, 12(9):12473–12488.

Ferreira, A., Correia, R., Brito, M., and Antunes, L. (2011). Usable access control policy and model for healthcare. In *Computer-Based Medical Systems (CBMS), 2011 24th International Symposium on*, pages 1–6. IEEE.

Garcia-Morchon, O. and Wehrle, K. (2010a). Efficient and context-aware access control for pervasive medical sensor networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on*, pages 322–327. IEEE.

Garcia-Morchon, O. and Wehrle, K. (2010b). Modular context-aware access control for medical sensor networks. In *Proceedings of the 15th ACM symposium on Access control models and technologies*, pages 129–138. ACM.

Gupta, S. K., Mukherjee, T., and Venkatasubramanian, K. (2006). Criticality aware access control model for pervasive applications. In *null*, pages 251–257. IEEE.

Haque, M. M., Pathan, A.-S., and Hong, C. S. (2008). Securing u-healthcare sensor networks using public key based scheme. In *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, volume 2, pages 1108–1111. IEEE.

He, D., Zeadally, S., Kumar, N., and Lee, J.-H. (2016). Anonymous authentication for wireless body area networks with provable security.

Huang, Y.-M., Hsieh, M.-Y., Chao, H.-C., Hung, S.-H., and Park, J. H. (2009). Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. *Selected Areas in Communications, IEEE Journal on*, 27(4):400–411.

Hughes, L., Wang, X., and Chen, T. (2012). A review of protocol implementations and energy efficient cross-layer design for wireless body area networks. *Sensors*, 12(11):14730–14773.

Khan, J. Y., Yuce, M. R., and Karami, F. (2008). Performance evaluation of a wireless body area sensor network for remote patient monitoring. In *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, pages 1266–1269. IEEE.

Khan, Z., Aslam, N., Sivakumar, S., and Phillips, W. (2012). Energy-aware peering routing protocol for indoor hospital body area network communication. *Procedia Computer Science*, 10:188–196.

Khan, Z. A., Sivakumar, S., Phillips, W., and Aslam, N. (2014). A new patient monitoring framework and energy-aware peering routing protocol (epr) for body area network communication. *Journal of Ambient Intelligence and Humanized Computing*, 5(3):409–423.

Khan, Z. A., Sivakumar, S., Phillips, W., and Robertson, B. (2013). A qos-aware routing protocol for reliability sensitive data in hospital body area networks. *Procedia Computer Science*, 19:171–179.

Kim, D.-Y. and Cho, J. (2009). Wban meets wban: smart mobile space over wireless body area networks. In *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, pages 1–5. IEEE.

Kumar, P. and Lee, H.-J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1):55–91.

Latré, B., Braem, B., Moerman, I., Blondia, C., and Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks*, 17(1):1–18.

Lee, Y. S., Alasaarela, E., and Lee, H. (2014). Secure key management scheme based on ecc algorithm for patient's medical information in healthcare system. In *The International Conference on Information Networking 2014 (ICOIN2014)*, pages 453–457. IEEE.

Lorch, M. and Kafura, D. (2002). Supporting secure ad-hoc user collaboration in grid environments. In *Grid ComputingGRID 2002*, pages 181–193. Springer.

Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., and Jamalipour, A. (2014). Wireless body area networks: a survey.

Movassaghi, S., Arab, P., and Abolhasan, M. (2012). Wireless technologies for body area networks: Characteristics and challenges. In *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, pages 42–47. IEEE.

Nazareth, S. and Smith, S. W. (2004). Using spki/sdsi for distributed maintenance of attribute release policies in shibboleth. In *ICWI*, pages 218–226.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., and Trombeta, A. (2010). Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 13(3):24.

OASIS (2005).

Otto, C., Milenkovic, A., Sanders, C., and Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4):307–326.

Parducci, B. (2005). extensible access control markup language (xacml) specification.

Patel, M. and Wang, J. (2010). Applications, challenges, and prospective in emerging body area networking technologies. *Wireless Communications, IEEE*, 17(1):80–88.

Razzaque, M. A., Hong, C. S., and Lee, S. (2011). Data-centric multiobjective qos-aware routing protocol for body sensor networks. *Sensors*, 11(1):917–937.

Rushanan, M., Rubin, A. D., Kune, D. F., and Swanson, C. M. (2014). Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE Symposium on Security and Privacy*, pages 524–539. IEEE.

Salehi, S. A., Razzaque, M., Naraei, P., and Farrokhtala, A. (2013a). Detection of sinkhole attack in wireless sensor networks. In *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*, pages 361–365. IEEE.

Salehi, S. A., Razzaque, M., Naraei, P., and Farrokhtala, A. (2013b). Security in wireless sensor networks: Issues and challanges. In *Space Science and Communication (IconSpace), 2013 IEEE International Conference on*, pages 356–360. IEEE.

Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000). The nist model for role-based access control: towards a unified standard. In *ACM workshop on Role-based access control*, volume 2000.

Seyedi, M., Kibret, B., Lai, D. T., and Faulkner, M. (2013). A survey on intrabody communications for body area network applications. *Biomedical Engineering, IEEE Transactions on*, 60(8):2067–2079.

Shaikh, F. K., Zeadally, S., and Exposito, E. (2015). Enabling technologies for green internet of things.

Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J., and Jeong, S.-P. (2015). Constructing rbac based security model in u-healthcare service platform. *The Scientific World Journal*, 2015.

Sohraby, K., Minoli, D., and Znati, T. (2007). *Wireless sensor networks: technology, protocols, and applications*. John Wiley & Sons.

Toninelli, A., Montanari, R., Kagal, L., and Lassila, O. (2006). A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In *The Semantic Web-ISWC 2006*, pages 473–486. Springer.

Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., and Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. *Journal of medical systems*, 36(3):1065–1094.

Ullah, S., Khan, P., Ullah, N., Saleem, S., Higgins, H., and Kwak, K. S. (2010). A review of wireless body area networks for medical applications. *arXiv preprint arXiv:1001.0831*.

Venkatasubramanian, K. K., Mukherjee, T., and Gupta, S. K. (2014). Caac–an adaptive and proactive access control approach for emergencies in smart infrastructures. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 8(4):20.

Wan, J., Ullah, S., Lai, C.-F., Zhou, M., Wang, X., et al. (2013). Cloud-enabled wireless body area networks for pervasive healthcare. *Network, IEEE*, 27(5):56–61.

Wang, C., Lu, W., Narayanan, M. R., Redmond, S. J., and Lovell, N. H. (2015). Low-power technologies for wearable telecare and telehealth systems: A review. *Biomedical Engineering Letters*, 5(1):1–9.

Wong, A. C. W., Dawkins, M., Devita, G., Kasparidis, N., Katsiamis, A., King, O., Lauria, F., Schiff, J., and Burdett, A. J. (2013). A 1 v 5 ma multimode ieee 802.15. 6/bluetooth low-energy wban transceiver for biotelemetry applications. *Solid-State Circuits, IEEE Journal of*, 48(1):186–198.

Xu, H. and Yang, L. (2008). Ultra-wideband technology: Yesterday, today, and tomorrow. In *Radio and Wireless Symposium, 2008 IEEE*, pages 715–718. IEEE.

Yuce, M. R. (2010). Implementation of wireless body area networks for healthcare systems. *Sensors and Actuators A: Physical*, 162(1):116–129.

Zhang, L., Ahn, G.-J., and Chu, B.-T. (2001). A rule-based framework for role based delegation. In *Proceedings of the sixth ACM symposium on Access control models and technologies*, pages 153–162. ACM.

Zhang, L., Ahn, G.-J., and Chu, B.-T. (2002). A role-based delegation framework for healthcare information systems. In *Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 125–134. ACM.

Zhang, L., Ahn, G.-J., and Chu, B.-T. (2003). A rule-based framework for role-based delegation and revocation. *ACM Transactions on Information and System Security (TISSEC)*, 6(3):404–441.

Zhang, M., Raghunathan, A., and Jha, N. K. (2014a). Trustworthiness of medical devices and body area networks.

Zhang, Z., Wang, H., Lin, X., Fang, H., and Xuan, D. (2013). Effective epidemic control and source tracing through mobile social sensing over wbans. In *INFOCOM, 2013 Proceedings IEEE*, pages 300–304. IEEE.

Zhang, Z., Wang, H., Wang, C., and Fang, H. (2014b). Cluster-based epidemic control through smartphone-based body area networks.

Zhao, N., Ren, A., Hu, F., Zhang, Z., Rehman, M. U., Zhu, T., Yang, X., and Alomainy, A. (2016). Double threshold authentication using body area radio channel characteristics. *IEEE Communications Letters*, 20(10):2099.

Zhou, H. (2012). *The internet of things in the cloud: A middleware perspective*. CRC press.